

**This Page Is Inserted by IFW Operations  
and is not a part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problems Mailbox.**

**THIS PAGE BLANK (USPTO)**



09 / 7 6 2 5 4 0

## MINISTERO DELL'INDUSTRIA, DEL COMMERCIO E DELL'ARTIGIANATO

DIREZIONE GENERALE DELLA PRODUZIONE INDUSTRIALE  
UFFICIO ITALIANO BREVETTI E MARCHI

IT 99/262



REC'D 10 SEP 1999

WIPO PCT

EJW

INV. IND.

Autenticazione di copia di documenti relativi alla domanda di brevetto per .....

N. .... RM98 A 000542

PRIORITY  
DOCUMENTSUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

*Si dichiara che l'unita copia è conforme ai documenti originali  
depositati con la domanda di brevetto sopraspecificata, i cui dati*

*risultano dall'accluso processo verbale di deposito* Inoltre;  
Verbale scioglimento riserve UPICA di Roma n° RM R 1099  
del 9.10.1998 contenente n°12 tavole di disegni definitivi.  
(Pag.13).

R ma, li 28 GIU. 1999

IL REGGENTE

IL DIRETTORE DELLA DIVISIONE

D.ssa Paola DI CINTIO

## AL MINISTERO DELL'INDUSTRIA DEL COMMERCIO E DELL'ARTIGIANATO

MODULO A

UFFICIO ITALIANO BREVETTI E MARCHI - ROMA

DOMANDA DI BREVETTO PER INVENZIONE INDUSTRIALE, DEPOSITO RISERVE, ANTICIPATA ACCESSIBILITÀ AL PUBBLICO



## A. RICHIEDENTE (I)

1) Denominazione ALASI di Arcieri Franco & C. s.a.s. SA  
 Residenza Austis (Nuoro), ITALIA codice 00915950919  
 2) Denominazione \_\_\_\_\_  
 Residenza \_\_\_\_\_ codice \_\_\_\_\_

## B. RAPPRESENTANTE DEL RICHIEDENTE PRESSO L'U.I.B.M.

cognome e nome de Benedetti Fabrizio ed altri cod. fiscale \_\_\_\_\_  
 denominazione studio di appartenenza SOCIETA' ITALIANA BREVETTI S.p.A.  
 via Piazza di Pietra n. 0039 città ROMA cap 00186 (prov) RM

## C. DOMICILIO ELETTIVO destinatario

via \_\_\_\_\_ n. \_\_\_\_\_ città \_\_\_\_\_ cap \_\_\_\_\_ (prov) \_\_\_\_\_

## D. TITOLO

classe proposta (sez/cl/scf) \_\_\_\_\_

gruppo/sottogruppo \_\_\_\_\_

"DISPOSITIVO DI CONTROLLO DI ACCESSI IN RETE TRAMITE IL RICONOSCIMENTO VELOCE DI TRAME APPLICATIVE CHE SODDISFANO UN INSIEME DI REGOLE PREDEFINITE"

ANTICIPATA ACCESSIBILITÀ AL PUBBLICO: SI ☐ NO ☒

SE ISTANZA: DATA \_\_\_\_\_

N° PROTOCOLLO \_\_\_\_\_

INVENTORI DESIGNATI cognome nome

cognome nome

1) ARCIERI Franco 3) TALAMO Maurizio  
 2) MARINELLI Guido Maria 4) \_\_\_\_\_

## F. PRIORITÀ

nazione o organizzazione

tipo di priorità

numero di domanda

data di deposito

allegato  
S/R

1) \_\_\_\_\_  
 2) \_\_\_\_\_

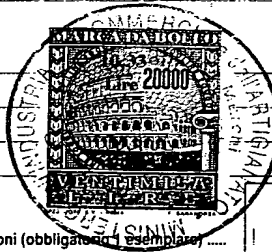
## SCIOGLIMENTO RISERVE

Data

N° Protocollo

## G. CENTRO ABILITATO DI RACCOLTA COLTURE DI MICRORGANISMI, denominazione

## H. ANNOTAZIONI SPECIALI



## DOCUMENTAZIONE ALLEGATA

N. es.

Doc. 1) 12 PROV n. pag. 85 riassunto con disegno principale, descrizione e rivendicazioni (obbligatorio 1 esemplare)  
 Doc. 2) 12 PROV n. tav. 12 disegno (obbligatorio se citato in descrizione, 1 esemplare)  
 3) 0 RIS lettera d'incarico, ~~prova di tecnica o di prodotto~~  
 Doc. 4) 0 RIS designazione inventore  
 Doc. 5) 0 RIS documenti di priorità con traduzione in italiano  
 Doc. 6) 0 RIS autorizzazione o atto di cessione  
 Doc. 7) 0 nominativo completo del richiedente

## SCIOGLIMENTO RISERVE

Data

N° Protocollo

confronta singole priorità

8) attestati di versamento, totale lire novecentoquindicimila=COMPILATO IL 12.08.1998 FIRMA DEL (I) RICHIEDENTE (I)CONTINUA S/NO NODEL PRESENTE ATTO SI RICHIEDE COPIA AUTENTICA S/NO SI

obbligatorio

Giorgio Strini  
 (Isr. Albo n. 452 BM)

UFFICIO PROVINCIALE IND. COMM. ART. DI

RM 98A 000542

ROMA codice 58

VERBALE DI DEPOSITO NUMERO DI DOMANDA

L'anno millenovecento novantottoil giorno dodicidel mese di agostoIl (i) richiedente (i) sopraindicato (i) ha (hanno) presentato a me sottoscritto la presente domanda, corredata di n. 00 fogli aggiuntivi per la concessione del brevetto soprariportato.

## I. ANNOTAZIONI VARIE DELL'UFFICIO ROGANTE

timbro  
O dell'ufficio

UFFICIALE ROGANTE

CESARE A. GASPERINI  
 Funzionario Camerale

RM 98 A 000542

SIB 91758

DESCRIZIONE dell'invenzione industriale dal titolo:

"DISPOSITIVO DI CONTROLLO DI ACCESSI IN RETE TRAMITE  
IL RICONOSCIMENTO VELOCE DI TRAME APPLICATIVE CHE  
SODDISFANO UN INSIEME DI REGOLE PREDEFINITE"

della ditta italiana ALASI di Arcieri Franco & C.  
s.a.s.

con sede in AUSTIS (NUORO) - ITALIA

-!-!-!-

DESCRIZIONE

La presente invenzione ha come oggetto un  
dispositivo di controllo di accessi in rete tramite il  
riconoscimento veloce di trame applicative che  
soddisfano un insieme di regole predefinite.

In particolare, il dispositivo secondo  
l'invenzione permette sia il rilevamento e  
l'interpretazione di protocolli applicativi di sistemi  
di trasmissione dati su rete sia il confronto di ogni  
trama di comunicazione rilevata ed interpretata con un  
insieme di "pattern" di controllo. Nel caso di trama  
riconosciuta, il dispositivo permette l'accesso al  
servizio. Nel caso di trama non riconosciuta, il  
dispositivo nega l'accesso al servizio.

Per "pattern" (o regola d'accesso) verrà intesa



S.I.B.  
ROMA

all'interno della presente descrizione la specifica di riconoscimento di una particolare trama di comunicazione.

Tale specifica verrà preferenzialmente intesa come un insieme di coppie <tipo di dato>/<valore dato> assunte dai campi all'interno della trama di comunicazione. Le coppie <tipo di dato>/<valore dato> sono specificate in base ai vari livelli di comunicazione che si trovano all'interno della trama di comunicazione sia per quanto concerne la parte di controllo sia anche per quanto concerne la parte di informazione. Nel corso della presente descrizione verranno illustrate, a titolo di esempio, trame di comunicazione di tipo HTTP (i servizi di browsing su Internet).

Dispositivi di controllo di accessi in rete sono noti e si possono suddividere in due grandi categorie:

- 1) In una prima categoria, le varie regole di accesso vengono rappresentate tramite matrici multidimensionali rappresentate in forma non-compressa, facendo uso di semplici linguaggi di accesso a tali matrici. Lo svantaggio di una tale rappresentazione è dato dalla notevole occupazione in memoria: una matrice 10-dimensionale con 100 elementi per dimensione ha una occupazione di memoria di  $100^{10}$ .

2) In una seconda categoria, le varie regole di accesso vengono rappresentate tramite matrici multidimensionali rappresentate in forma compressa. L'accesso a tali matrici non è di tipo diretto. Una tale modalità presenta lo svantaggio di richiedere l'utilizzo di linguaggi ad alto livello i quali, mediante operatori di test e di confronto, determinano la particolare procedura da attivare in risposta al riconoscimento di una regola d'accesso. Le particolari strutture di controllo così utilizzate appesantiscono il processo di interpretazione, rendendolo inefficiente. Risulta peraltro difficile, se non impossibile, la realizzazione di metodi generalizzati per il riconoscimento delle strutture informative su tecnologie veloci (firmware).

In ambedue le tipologie di dispositivi di tecnica nota sussiste poi l'ulteriore svantaggio che il riconoscimento delle trame di comunicazione non può essere basato su un qualsiasi componente della trama, ma solamente su trame a livello non applicativo.

La presente invenzione ovvia a tali problemi di tecnica precedente, in quanto prevede un dispositivo di controllo di accessi in rete tramite il riconoscimento deterministico di trame applicative che soddisfano un insieme di regole predefinite

comprendente:

- mezzi di rilevamento ed interpretazione delle trame applicative da riconoscere;
- mezzi di memorizzazione di regole predefinite;
- mezzi di compilazione delle regole predefinite in una struttura dati ad accesso diretto;
- mezzi di memorizzazione di detta struttura dati ad accesso diretto; e
- mezzi di confronto tra le trame applicative da riconoscere e detta struttura dati ad accesso diretto, in cui il riconoscimento può essere effettuato su qualsiasi componente della trama ed in cui la struttura dati ad accesso diretto permette di ottenere un tempo di accesso sostanzialmente indipendente dalla numerosità delle regole.

Come noto, una struttura dati ad accesso diretto ha la proprietà di consentire l'accesso all'elemento  $i$ -esimo senza dover necessariamente accedere preventivamente agli elementi precedenti, come avviene invece nel caso di strutture dati ad accesso sequenziale. Esempi noti di strutture dati ad accesso diretto sono i vettori, le matrici, le tavole di corrispondenza, la memoria di un elaboratore etc.

Un primo vantaggio del dispositivo di controllo di accessi secondo la presente invenzione è dato dalla

flessibilità con la quale è possibile realizzare un pattern di riconoscimento. Grazie all'utilizzo dell'apparecchio per il rilevamento e l'interpretazione di protocolli applicativi, spiegato in dettaglio nel seguito, il riconoscimento delle trame di comunicazione può essere infatti basato su una qualsiasi componente della trama, sia sulla parte controllo che sulla parte informazione. E' quindi possibile realizzare pattern di riconoscimento (e quindi limitare l'accesso) in base ai contenuti informativi scambiati e non soltanto in base agli indirizzi ed ai servizi di rete utilizzati.

Un secondo vantaggio del dispositivo secondo la presente invenzione è dato dalla sua capacità di gestire un elevatissimo numero di pattern (dell'ordine dei milioni) senza alcun degrado delle prestazioni.

In un contesto nel quale siano coinvolti un numero elevato di utenti, di server e di servizi applicativi sui server stessi, quando si vuole gestire in modo diretto l'accessibilità di ogni utente al singolo server e servizio applicativo da questo reso disponibile ci si trova infatti in presenza di una crescita quadratica dei pattern. Ad esempio, dati 1000 utenti sul territorio e 100 server ed ai quali si vuole gestire e controllare gli accessi vengono generati



S.I.B.  
ROMA

$1000 \times 100 = 100.000$  pattern. Questo numero aumenta ancora nel caso in cui si voglia gestire e controllare l'accesso alle applicazioni per ogni singolo server, rendendo, in casi reali su organizzazioni medio/grandi, il numero di pattern stimabile nell'ordine dei milioni.

Tale numero di pattern è del tutto accettabile per il dispositivo di cui alla presente invenzione.

Il riconoscimento delle trame di comunicazione acquisite è infatti basato su un algoritmo deterministico (quindi né euristico né probabilistico) di accesso in grado di garantire un tempo di accesso costante ed indipendente (sotto qualsiasi input) dal numero dei pattern.

Per ogni trama correttamente riconosciuta, il dispositivo di controllo di accessi esegue poi l'operazione di coordinamento associata al riconoscimento. A riconoscimento avvenuto infatti, il dispositivo attiverà una comunicazione a livello TCP/IP (o livelli corrispondenti di altri protocolli) con l'applicazione server individuata come risultato del riconoscimento, anche parziale, della componente informativa della trama di ingresso, fornendo come parametri parte della componente informativa già riconosciuta oppure non ancora processata. Le modalità

di invio (formato di invio dei parametri, numero dei parametri da inviare, applicazione da attivare etc.) sono associate all'azione di riconoscimento e sono quindi memorizzate nei pattern.

Il dispositivo di controllo di accessi secondo la presente invenzione può essere configurato per operare tanto in logica diretta che in logica negata.

In logica diretta saranno considerate accettate, e quindi portate a destinazione, tutte le trame che soddisfano i pattern di riconoscimento.

In logica negata saranno considerate accettate, e quindi portate a destinazione, tutte le trame che non soddisfano i pattern di riconoscimento. Tutte le trame riconosciute non saranno portate a destinazione.

La presente invenzione verrà qui di seguito descritta tramite una sua forma di realizzazione preferita, illustrata a scopo esemplificativo e non limitativo. Verrà fatto riferimento alle figure dei disegni allegati, in cui:

la figura 1 mostra un diagramma schematico dello standard OSI;

la figura 2 mostra una rappresentazione schematica del tipo di dati utilizzati nelle comunicazioni su rete;

la figura 3 mostra una rappresentazione

schematica del tipo di dati utilizzati nelle comunicazioni su rete con riferimento al protocollo TCP/IP;

la figura 4 mostra uno schema a blocchi dell'apparecchio di rilevamento ed interpretazione facente parte del dispositivo di controllo di accessi secondo la presente invenzione;

la figura 5 mostra uno schema di flusso che spiega il funzionamento della componente di figura 4;

le figure 6 e 7 mostrano ulteriori schemi di flusso per la comprensione di quanto descritto con riferimento alla figura 5;

le figure 8A e 8B mostrano un esempio di albero applicativo arricchito di informazioni di tipo statistico ottenuto tramite la componente di figura 4;

la figura 9 mostra uno schema a blocchi del dispositivo di controllo di accessi secondo la presente invenzione;

le figure 10A e 10B mostrano schemi esemplificativi della corrispondenza logica tra grafo bipartito e matrice bidimensionale;

la figura 11 contiene un esempio di specifica di regole predefinite; e

la figura 12 mostra una rappresentazione in forma matriciale di sequenze di identificatori numerici.

La trasmissione di dati da un dispositivo di sorgente ad un dispositivo di destinazione può avvenire secondo modalità differenti. Al fine di assicurare uno scambio di dati con una ampia probabilità di mancanza di errori è però necessario adottare un insieme di regole o procedure di controllo. Tali regole o procedure sono note con il termine di "protocolli di comunicazione".

Un protocollo standard di comunicazione è l'"Open System Interconnection" (OSI) della International Standards Organization (ISO). Tale protocollo è organizzato secondo una suddivisione in sette livelli, mostrata in figura 1. Il livello 7 (applicazione) del lato sorgente contiene informazioni relative al semplice messaggio (M) da inviare verso il lato destinazione. I successivi livelli del lato sorgente aggiungono informazioni di controllo al messaggio: il livello 6 (presentazione) suddivide i dati del messaggio originale in blocchi (M1 ed M2); il livello 5 (sessione) aggiunge un titolo (S) per indicare il mittente, il destinatario ed alcune informazioni relative alla sequenza; il livello 4 (trasporto) aggiunge informazioni (T) relative alla connessione logica tra il mittente ed il destinatario; il livello 3 (rete) aggiunge informazioni relative al percorso



(N) ed il messaggio viene suddiviso in pacchetti che rappresentano l'unità standard di comunicazione in una rete; il livello 2 (collegamento dati) aggiunge una parte di titolo (B) ed una parte di coda (E) al messaggio per assicurare il corretto ordine dei vari pacchetti e correggere errori di trasmissione; i singoli bit del messaggio e delle informazioni di controllo via via aggiunte dai vari livelli vengono trasmessi sul mezzo fisico attraverso il livello 1. La freccia F1 verso il basso sul lato sorgente indica le modalità secondo le quali viene costruito il messaggio in partenza. Tutte le aggiunte al messaggio vengono verificate e rimosse dal corrispondente livello dal lato del destinatario. La freccia F2 verso l'alto sul lato destinatario indica le modalità secondo le quali viene ricostruito il messaggio in arrivo.

Facendo riferimento allo standard OSI, l'unità di comunicazione in una rete è il pacchetto. I pacchetti solo a loro volta suddivisi in frame. L'inizio e la fine di ciascun frame vengono in genere stabiliti tramite caratteri di delimitazione. I frame sono a loro volta suddivisi in frame di informazione e frame di controllo. I frame di informazione servono al trasporto di dati relativi al messaggio da trasmettere lungo la rete, mentre i frame di controllo servono a

gestire le modalità secondo le quali tale trasporto deve avvenire, vale a dire al controllo del flusso ed all'attivazione delle azioni di recupero degli errori. Sia i frame di informazione che i frame di controllo contengono una parte di intestazione che identifica il tipo di frame ed una parte di corpo tipica invece del frame stesso.

La struttura dei frame di informazione verrà descritta facendo riferimento alla figura 2. Nella parte superiore di tale figura è rappresentata in maniera schematica la struttura generica di un pacchetto di livello OSI 2, comprendente cioè sia frame di informazione 1 che frame di controllo 2. La costituzione di un singolo frame di informazione (livello OSI 3) indica la presenza di una parte di intestazione 3, che contiene l'identificazione che il frame in oggetto è un frame di informazione, e di una parte di corpo 4. La parte di corpo (livelli OSI 4-7) contiene il messaggio 5 vero e proprio, unitamente ad una serie 6 di campi, rappresentati in maniera esemplificativa in figura con i caratteri C1, C2 e C3, tipici della particolare sintassi applicativa utilizzata. Per sintassi applicativa si intendono le informazioni relative al numero di campi contenuti all'interno della serie 6, al significato di ciascuno

di tali campi ed ai dati in essi contenuti.

Il modello OSI fin qui schematicamente riassunto è solamente un modello concettuale. Uno dei protocolli attualmente più utilizzati ed universalmente accettati è il protocollo TCP/IP (Transmission Control Protocol and Internet Protocol). Tale protocollo, come anche altri protocolli di comunicazione adottati, è spiegabile tramite riferimenti alla struttura a livelli del modello OSI. In ciascuno di tali protocolli infatti, un determinato livello di sorgente suddividerà i dati che riceve da un livello superiore aggiungendo agli stessi una intestazione e/o una coda per poi passare il tutto ad un livello inferiore. Dal lato destinazione avverranno le operazioni inverse.

Con riferimento alla successiva figura 3, viene mostrata una rappresentazione schematica del tipo di dati utilizzati nelle comunicazioni su rete locale con riferimento al protocollo TCP/IP trasportante il servizio applicativo HTTP (browsing su Internet).

Il livello Ethernet comprende sostanzialmente quattro tipi di campi:

- un campo 101 di indirizzo della scheda di rete di destinazione;
- un campo 102 di indirizzo della scheda di rete di sorgente;

- un campo 103 indicativo del protocollo di comunicazione trasportato, in questo caso indicativo del protocollo IP e della lunghezza della parte informazione; e

- un campo informazione 104, contenente cioè i dati del livello Ethernet, vale a dire tutta la struttura del protocollo IP trasportato.

Il livello IP (incapsulato nel livello Ethernet) comprende sostanzialmente sei tipi di campi:

- una serie di campi di controllo 105 identificativi della versione, della lunghezza, delle opzioni di trasmissione, filler etc.;

- un campo 106 indicativo del protocollo di comunicazione trasportato, in questo caso indicativo del protocollo TCP;

- un campo 107 di indirizzo IP di destinazione, vale a dire l'indirizzo IP di chi deve ricevere il pacchetto;

- un campo 108 di indirizzo IP di sorgente, vale a dire l'indirizzo IP di chi ha inviato il pacchetto; e

- un campo informazione 109, contenente cioè i dati del livello IP, vale a dire tutta la struttura del protocollo TCP trasportato.

Il livello TCP (incapsulato nel livello IP) comprende quattro tipi di campi:

- un campo porta di sorgente 110, indicante la porta



di servizio TCP utilizzata da chi ha inviato il pacchetto;

- un campo porta di destinazione 111, indicante la porta di servizio TCP utilizzata dal ricevitore del pacchetto;

- una serie di campi di controllo 112 identificanti l'ID di pacchetto, la finestra di lavoro, il crc, opzioni varie etc.; e

- un campo di informazione 113, contenente cioè i dati del livello TCP, vale a dire tutta la struttura del servizio applicativo HTTP trasportato, cioè i comandi del linguaggio HTTP e, nella sua parte informativa, i comandi del linguaggio HTML.

Sistemi di rilevamento dei dati trasmessi tra un nodo sorgente ed un nodo di destinazione sono già noti. Tali sistemi si limitano però all'analisi dei livelli OSI 2 (collegamento dati) e OSI 3 (rete). Il rilevamento e la successiva interpretazione dei dati a tali livelli permettono soltanto l'individuazione di anomalie nel protocollo di scambio tra i vari componenti di un sistema di trasmissione dati su rete.

Uno svantaggio tipico di tali sistemi di tecnica precedente è pertanto l'impossibilità di decodificare l'informazione di tipo applicativo trasportata sulla rete, vale a dire l'informazione relativa ai livelli

4-7 dello standard OSI.

Nelle successive figure da 4 ad 8B verranno descritte nel dettaglio la struttura ed il funzionamento di un apparecchio per il rilevamento e l'interpretazione di protocolli applicativi.

Verrà fatto ora riferimento alla figura 4, che mostra uno schema a blocchi dell'apparecchio. In tale figura vengono innanzitutto mostrati un nodo di sorgente 7 ed un nodo di destinazione 8, terminali del tratto di rete i cui dati vengono rilevati ed interpretati. Lungo il collegamento tra tali due nodi, rappresentato schematicamente dalle frecce F3, F4, F5, F6 e dal mezzo trasmissivo 23, viaggiano in maniera bidirezionale dati relativi a più comunicazioni tra un primo insieme di elaboratori di sorgente (non indicati in figura) a monte del nodo di sorgente 7 ed un secondo insieme di elaboratori di destinazione (non indicati in figura) a valle del nodo di destinazione 8.

Tali dati vengono rilevati tramite un dispositivo 9 di rilevamento dati. Diversi sono i dispositivi di rilevamento del tipo noti sul mercato; per quanto riguarda le reti basate su tecnologia Ethernet è ad esempio possibile citare la scheda Fast Etherlink XL™ della ditta 3Com™. Per quanto riguarda le reti basate

su tecnologia X.25 è possibile citare ad esempio la scheda S508 della ditta canadese Sangoma™. Tale scheda può operare con diversi standard a livello OSI 1 (livello fisico) quali ad esempio lo standard RS232 (o V.24) e lo standard RS422 (o V.35). Gli standard di livello OSI 2 (collegamento dati) con i quali tale scheda può operare sono ad esempio lo standard HDLC oppure, contenuto in questo, lo standard X.25. Il tipo di dispositivo di rilevamento 9 da scegliersi ai fini della presente invenzione potrà comunque variare a seconda degli standard di livello OSI 1 o OSI 2 sui quali si desidera operare. Sarà infatti possibile pensare di utilizzare dispositivi di rilevamento che operino con standard implementativi differenti del livello OSI 2, quali ad esempio il "Frame Relay" o lo SDLC o ancora il BSC o altri similari. Tali dispositivi sono comunque ben noti all'esperto del ramo e non verranno qui discussi in dettaglio.

Il rilevamento avviene in maniera "trasparente" tramite due connettori paralleli 10 ed 11, indicati schematicamente in figura, atti a permettere il rilevamento dei dati provenienti rispettivamente dal nodo di sorgente 7 e dal nodo di destinazione 8. Il dispositivo di rilevamento 9, mostrato nel suo complesso nel blocco indicato a tratteggio in figura,

è tale da comprendere un ricevitore dei dati di sorgente 12, un ricevitore dei dati di destinazione 13 ed una interfaccia di connessione 14. Il ricevitore dei dati di sorgente 12 è tale da permettere la ricezione dei soli dati provenienti dal nodo di sorgente 7 secondo quanto schematicamente indicato dalla freccia F7; il ricevitore dei dati di destinazione 13 è tale invece da permettere la ricezione dei soli dati provenienti dal nodo di destinazione 8 secondo quanto schematicamente indicato dalla freccia F8. I dati così ricevuti vengono trasmessi alla interfaccia di connessione 14, secondo quanto indicato dalle frecce F9 ed F10.

Ciascun pacchetto di dati ad un livello corrispondente al livello OSI 2 letto tramite l'unità di rilevamento 9 viene inviato ad una unità di controllo 15, come indicato dalla freccia F11. L'unità di controllo 15 verrà descritta oltre in dettaglio. A ciascuno di tali pacchetti viene associato un istante temporale di lettura tramite una unità 16 di datazione, rappresentata per comodità di presentazione all'esterno dell'unità di controllo 15 e collegata a quest'ultima come indicato tramite la freccia F12. Tale unità 16 di datazione può essere un qualsiasi dispositivo a tempo assoluto presente in commercio, in



particolare via radio o satellitare. Nella modalità di realizzazione preferita delle presente invenzione si è utilizzato un orologio digitale radiocontrollato che si tara sull'ora CET (Central European Time) irradiata tramite satellite geostazionario.

Successivamente all'associazione dell'istante temporale di lettura tramite l'unità 16 di datazione, l'unità di controllo 15 provvede a riordinare logicamente i singoli frame in modo da ricostruire l'esatta sequenza logico/temporale di spedizione dei frame che, come noto, non sempre coincide con la sequenza di ricezione: è infatti possibile, causa le tecniche di instradamento su reti di telecomunicazione, che una sequenza di spedizione del tipo "ABC" possa essere ricevuta in tutte e sei le sue possibili combinazioni, vale a dire "ABC", "ACB", "BAC", "BCA", "CAB", "CBA". L'unità di controllo 15 provvede quindi alla discriminazione dei frame di informazione dai frame di controllo. Nel caso in cui l'informazione venga ad esempio trasmessa in HDLC, l'ultimo bit della parte di intestazione di un frame di informazione è 0 mentre l'ultimo bit della parte di intestazione di un frame di controllo è 1. All'interno dell'unità di controllo 15 sono pertanto presenti mezzi, non indicati in figura, atti alla

discriminazione di tale ultimo bit, ad esempio un firmware contenuto in una ROM. In ogni caso, qualunque sia il codice di trasmissione dati utilizzato, saranno sempre note le modalità che distinguono un frame di controllo da un frame di informazione. Sarà pertanto sempre possibile prevedere mezzi atti a tale discriminazione. Tale discriminazione consente pertanto di immagazzinare i singoli frame di informazione privi della parte di intestazione e comprendenti la sola parte di corpo, contenente cioè le informazioni tipiche della particolare sintassi applicativa utilizzata, ed il messaggio da trasmettere.

I dati incorporanti l'istante temporale di rilevamento e suddivisi in frame di informazione e frame di controllo vengono immagazzinati all'interno di una unità 17 di memorizzazione dei dati rilevati, collegata in maniera bidirezionale all'unità di controllo 15 come rappresentato tramite la freccia F13. E' poi presente una unità 18 di memorizzazione di dati predeterminati, collegata in maniera bidirezionale all'unità di controllo 15. Tali dati predeterminati rappresentano possibili interpretazioni dei frame di informazione o di controllo contenuti nell'unità di memorizzazione 17. Il loro utilizzo

verrà spiegato in seguito con riferimento alle successive figure. Il collegamento tra l'unità di memorizzazione 18 e l'unità di controllo 15 è rappresentato tramite la freccia F14.

Verrà fatto successivamente riferimento alla figura 5, che mostra uno schema di flusso indicante le operazioni che vengono effettuate dall'unità di controllo 15 sui frame di informazione immagazzinati nell'unità 17 di memorizzazione. E' da intendersi che l'accesso a tale frame potrà eventualmente essere selettivamente regolato tramite sistemi di gestione privilegi ed autorizzazioni quali ad esempio password, codici di criptazione, deciptazione, lettori di badge e similari in possesso di utenti abilitati, a seconda dei casi.

Un primo passo S1 indica la lettura dei vari pacchetti avvenuta tramite l'unità 3 di rilevamento. Un secondo passo S2 indica la distinzione, precedentemente descritta, che l'unità di controllo 15 effettua tra i frame di informazione ed i frame di controllo, unitamente all'associazione dell'istante temporale di rilevamento.

Sui frame di controllo, di basso livello (non applicativo), il cui utilizzo è marginale ai fini della presente invenzione, potrà comunque essere

prevista una elaborazione statistica, effettuata nel passo S3. Tale elaborazione non viene qui descritta in dettaglio; le modalità con le quali essa avviene risulteranno chiare in seguito. Il risultato finale di una tale elaborazione fornirà una elencazione dei vari frame di controllo, riportando inoltre il conteggio del numero di occorrenze di ciascuno di tali frame.

Per quanto concerne i frame di informazione, il flusso procede verso un passo S4 in cui i singoli frame di informazione vengono ricostruiti in base alla sintassi applicativa specifica degli stessi. Ai fini di tale ricostruzione, le strutture di sintassi applicativa dei singoli frame di informazione devono essere note. Esse sono infatti contenute all'interno dell'unità 18 di memorizzazione di dati predeterminati descritta con riferimento alla precedente figura 3. Tale unità 18 contiene, ad esempio in un "file" di testo, una descrizione formale astratta di possibili interpretazioni dei frame di informazione o di controllo. Tali dati rappresentano le modalità secondo le quali può essere strutturata la parte di corpo di un singolo frame di informazione, ad esempio il codice di trasmissione macchina (vale a dire relativo ad un frame di informazione spedito dalla sorgente oppure dal destinatario), il numero di canale (vale a dire



relativo ad uno specifico elaboratore a monte del nodo di sorgente oppure ad uno specifico elaboratore a valle del nodo di destinazione), numeri di protocollo, numeri meccanografici etc. E' da intendersi che tale unità 18 può contenere sintassi di molteplici protocolli applicativi, dei frame di informazione da ricostruire in quel momento.

Tramite un confronto sequenziale della parte di corpo di ciascun frame di informazione con ciascuna delle tipologie astratte presenti nell'unità 18, si ottiene una ricostruzione dei singoli frame di informazione.

Successivamente a ciò, si è in grado di ricomporre le varie sequenze applicative intercorse tra un determinato elaboratore di sorgente ed un determinato elaboratore di destinazione, vale a dire un ordinamento temporale e secondo il tipo di comunicazione. Per sequenza applicativa verrà inteso nel corso della presente descrizione l'insieme dei frame di informazione scambiati tra un determinato elaboratore di sorgente ed un determinato elaboratore di destinazione all'interno di una singola comunicazione. La sequenza applicativa ordinata all'interno del passo S5 conterrà i singoli frame di informazione ordinati solamente secondo un criterio

temporale e non anche secondo un criterio logico. L'ordinamento temporale è stato reso possibile dall'associazione dell'istante temporale avvenuta nel precedente passo S2.

Ai fini di un ordinamento anche logico dei dati all'interno di una specifica sequenza applicativa può rivelarsi utile, ma non necessaria, la presenza di un insieme di regole applicative che governano lo scambio di dati tra sorgente e destinazione. Tali regole applicative, tipiche della particolare tipologia di colloquio tra un determinato elaboratore di sorgente ed un determinato elaboratore di destinazione, devono essere predefinite e come tali sono anch'esse raccolte nell'unità 18 di memorizzazione di dati predeterminati. Tali regole applicative sono un insieme di possibili interpretazioni di sequenze di frame di informazione contenuti nell'unità di memorizzazione 17 dei dati rilevati.

Un esempio di regole applicative è dato dalla seguente tabella 1, in cui si fa riferimento ad una comunicazione tra una sorgente che rappresenta uno studente (client) che voglia effettuare una iscrizione via terminale all'università, ed un destinatario (server) che rappresenta l'università cui lo studente vuole iscriversi.

TABELLA 1

1: AS ? FDB 15 AS ? FDB 5 AS ? FDB 0 La prenotazione dell'iscrizione è stata acquisita regolarmente
2: AS ? FDB 13 AS ? FDB 0 La posizione dell'utente non è regolare
.....
.....
.....

Ogni riga di tale tabella è una regola applicativa, indicante cioè una possibile sequenza applicativa di scambio dati tra sorgente e destinatario. Viene qui di seguito riportato il significato di ciascuna di tali sequenze applicative. La prima riga indica ad esempio la seguente sequenza di frame di informazione:

- la sorgente (AS) interroga (?) il destinatario;
- il destinatario (FDB) risponde con l'attività numero 15;
- la sorgente (AS) interroga (?) nuovamente il destinatario;
- il destinatario (FDB) risponde con l'attività numero 5;
- la sorgente (AS) interroga (?) il destinatario; e

- il destinatario (FDB) risponde con l'attività numero 0.

Il risultato cui si perviene al termine di tale conversazione è che la prenotazione dell'iscrizione all'università è stata acquisita regolarmente.

La tabella 1, meramente esemplificativa, potrebbe essere anche rappresentata tramite una struttura ad albero con più o meno ramificazioni, a seconda del numero di sequenze applicative previste. Ogni percorso fino ad una delle foglie dell'albero rappresenterebbe una particolare sequenza applicativa, vale a dire una particolare conversazione tra sorgente e destinatario, vale a dire ancora una particolare sequenza di frame di informazione tra sorgente e destinatario.

Le regole applicative possono essere in numero qualunque. Maggiore sarà il numero di regole applicative fornito, maggiore sarà la possibilità di associare a ciascuna delle sequenze applicative temporalmente ricostruite nel passo S5 un significato logico ben definito, riscontrato tramite confronto con una particolare regola applicativa contenuta nell'unità di memorizzazione 18 di figura 3. In tale modo sarà dunque possibile verificare correttezza o anomalia della particolare sequenza applicativa in quel momento confrontata.



Nel passo S6 di figura 5 l'unità di controllo 15 verifica innanzitutto se tali regole applicative siano disponibili o meno. Supponendo che tali regole applicative siano note, il flusso può procedere o verso un passo S8 oppure verso un passo S9, a seconda di quanto scelto nel passo S7. Il passo S8 permette una semplice classificazione delle sequenze applicative. Ciascuna sequenza applicativa viene infatti classificata come appartenente ad un particolare percorso tra i vari percorsi possibili all'interno dell'albero delle regole applicative. Il passo S8 verrà spiegato in maggiore dettaglio con riferimento alla successiva figura 6.

Nel passo S9 invece, viene ricostruito il percorso logico di tutte le sequenze applicative rilevate dall'apparecchio in un predeterminato intervallo temporale. Tale passo S9 verrà spiegato in maggiore dettaglio con riferimento alla successiva figura 7.

L'apparecchio secondo la presente invenzione consente di effettuare una ricostruzione del percorso logico delle sequenze applicative anche nel caso in cui non sia previsto un insieme di regole applicative. Il flusso procede in tale caso verso un passo S10, anch'esso successivamente descritto.

Verrà fatto ora riferimento alla figura 6, che spiega in maggiore dettaglio quanto sopra descritto con riferimento al passo S8 di figura 5. In un primo passo S11 viene selezionata la singola sequenza applicativa oggetto del confronto. In un successivo passo S12 vengono selezionati, all'interno della sequenza applicativa selezionata, gli elementi caratterizzanti ai fini del confronto.

Nel caso esemplificativo precedentemente descritto di iscrizione all'università con riferimento alla tabella 1 tali elementi caratterizzanti potranno essere: l'identificativo dell'elaboratore di sorgente, l'identificativo dell'utente che ha richiesto l'operazione di iscrizione, i dati forniti dalla sorgente ed i dati forniti dal destinatario.

Nel passo S13 gli elementi caratterizzanti della sequenza applicativa in oggetto vengono confrontati con una delle regole applicative di cui alla precedente tabella 1 alla ricerca di una possibile corrispondenza. Nel caso in cui tale corrispondenza sia stata trovata, il flusso procede verso un passo S14 in cui tale corrispondenza viene segnalata e della quale andrà tenuto conto nei risultati dell'interpretazione. Il flusso torna poi a selezionare una successiva sequenza e a rieseguire il

passo S11. Nel caso in cui la corrispondenza di cui al passo S13 non sia stata trovata, l'unità di controllo 15 passa ad una successiva regola nel passo S15 e nel caso in cui (passo S16) vi siano ancora regole con le quali effettuare il confronto l'unità di controllo ritorna ad eseguire il confronto di cui al passo S13. Nel caso in cui invece non vi siano regole ulteriori, l'unità di controllo segnala una anomalia nel passo S17. Una tale anomalia può alternativamente significare:

- un tipo di sequenza che non sarebbe dovuto avvenire (anomalia vera e propria); oppure
- un tipo di sequenza non inserito per errore all'interno dell'albero delle regole applicative.

In ciascuno di tali casi il riscontro di una tale anomalia è sicuramente utile ai fini della certificazione delle tipologie di sequenze applicative intercorse nel tratto di rete posto sotto osservazione.

Verrà fatto ora riferimento alla successiva figura 6 che spiega in maggiore dettaglio quanto descritto nel passo S9 di figura 5.

I passi S18 ed S19 servono rispettivamente a selezionare la singola sequenza applicativa e gli elementi caratterizzanti della stessa, similmente a

quanto descritto con riferimento alla precedente figura 5. Il passo S20 serve ad indicare il confronto tra la sequenza applicativa e le regole applicative predefinite contenute all'interno dell'unità 18 di memorizzazione di dati predeterminati. Nel caso in cui si sia trovata una corrispondenza, il flusso procede verso un passo S21 in cui viene tenuto conto della corrispondenza rinvenuta tramite aggiornamento dei relativi campi statistici. I passi S18-S20 verranno successivamente ripetuti, fino ad esaurimento delle sequenze da classificare. Nel caso in cui invece non vengano trovate corrispondenze, la sequenza applicativa da classificare è nuova; essa può rappresentare una anomalia oppure semplicemente una sequenza che non è stata prevista. In questo caso il flusso procede verso un passo S22 in cui vengono inizializzati i campi statistici relativi a quella specifica sequenza. La sequenza riscontrata potrà inoltre inserita nella lista delle sequenze predefinite che servono ad effettuare la comparazione nel passo S20. Tale fatto è anche indicato dal doppio senso della freccia F14 della precedente figura 4. E' da intendersi che tali sequenze particolari, le probabili anomalie cioè, possono eventualmente essere marcate in maniera particolare in modo da essere



riconosciute come tali. Successivamente a ciò vengono anche in questo caso ripetuti i passi S18-S20 fino ad esaurimento delle sequenze da classificare. In particolare, oltre a poter individuare il numero di attraversamenti di ciascun ramo dell'albero, sarà possibile individuare anche rami non percorsi.

Nel caso in cui non sia presente una sequenza predefinita di regole applicative, l'unità di controllo sarà sempre in grado di effettuare una ricostruzione delle comunicazioni applicative intercorse sul tratto di rete sotto esame (passo S9 di figura 5). In tale caso ciascuna sequenza applicativa analizzata verrà confrontata non con sequenze predefinite, bensì con le sequenze precedentemente analizzate. L'albero applicativo arricchito di informazioni di tipo statistico verrà pertanto ricostruito tramite confronto reciproco di ciascuna parte di corpo dei frame di informazione con le altre. Verrà anche in questo caso formato un albero e sarà possibile conoscere il numero di attraversamenti di ciascun ramo. In questo caso non sarà ovviamente possibile individuare rami non percorsi, in quanto non si sarà a priori a conoscenza dell'esistenza di tali rami.

Verrà fatto ora riferimento alle figure 8A e 8B

che mostrano rispettivamente una struttura esemplificativa di frame informativo ed una struttura esemplificativa di albero applicativo arricchito di informazioni di tipo statistico ottenuta tramite l'apparecchio secondo la presente invenzione.

In figura 8A è possibile scorgere quattro campi differenti: un primo campo 19 che indica il nominativo dell'elaboratore di sorgente o dell'elaboratore di destinazione; un secondo campo 20 che indica il numero di collegamenti all'interno dell'intervallo di tempo di rilevamento, un terzo campo 21 che indica la durata media di ciascun collegamento, ad esempio in millisecondi, ed un quarto campo 22 che indica il codice dell'attività svolta.

La figura 8B indica l'albero ricostruito. Un primo elemento E1 dell'albero indica che AS (sorgente) si è collegato 20 volte, con una durata media di collegamento di 0 millisecondi (semplice apertura del collegamento con il destinatario) e ha effettuato l'attività con il codice 0. Un secondo elemento E2, unico "figlio" di E1, indica che in tutti e 20 questi collegamenti FDB (destinatario) ha risposto con l'attività con il codice 20, con una durata media di collegamento di 20 millisecondi. Due sono state le modalità con le quali si è proseguito. Per 18 volte

(elemento E3) AS ha risposto con l'attività 0 e per due volte (elemento E4) AS ha risposto con l'attività 1. L'albero prosegue con altri elementi, il cui significato risulta ora chiaro dal contesto. L'albero qui presentato è il risultato dell'ordinamento logico effettuato nei passi S9 o S10 della figura 5.

Si fa notare che l'individuazione dei contenuti del campo 19 e del campo 22 di ciascun elemento è stata effettuata tramite il passo S4 di figura 5. L'individuazione dei collegamenti tra i vari elementi, vale a dire il fatto che l'elemento E2 è "figlio" di E1 e che gli elementi E3 ed E4 sono "figli" di E2 è stata fatta o nel passo S9 oppure nel passo S10 di figura 5.

Terminata la descrizione dettagliata di un apparecchio per il rilevamento e l'interpretazione di protocolli applicativi su rete, verranno qui di seguito descritte in dettaglio la struttura ed il funzionamento delle rimanenti componenti del dispositivo di controllo di accessi secondo la presente invenzione.

Le modalità di connessione preferita di tale dispositivo sono in serie, su reti Ethernet da 10 Mbits (connettori rj58 e rj45) e 100 Mbits (rj45).

I protocolli di livello OSI 2 supportati saranno

tutti i protocolli incapsulati in Ethernet, quali 802.3, DOD IP, ARP etc.

I protocolli di livello OSI 3 supportati saranno tutti i protocolli incapsulati nei vari protocolli di livello OSI 2, quali TCP in IP, UDP in IP, Netbios in IEEE 802.3, SNA in IEEE 802.3 etc.

Verrà fatto innanzitutto riferimento alla figura 9, che mostra uno schema a blocchi del dispositivo di controllo di accessi secondo la presente invenzione. I vari blocchi di figura 9 verranno qui di seguito descritti uno alla volta.

*Elemento 201:*

E' l'elemento di memorizzazione delle regole di riconoscimento dei pattern. L'archivio delle regole di riconoscimento è formato leggendo un file oppure ad esempio digitando direttamente le regole tramite tastiera.

Si supporrà inizialmente che tali regole di riconoscimento si presentano quali coppie <tipo di dato>/<valore dato>.

Un pattern per il riconoscimento di una richiesta di browsing Internet da parte di un client con indirizzo 192.23.40.1 verso un server web di indirizzo 210.20.20.6 presenta ad esempio la seguente struttura:  
(ETH\_PROT, IP),



```
(IP_SRC_ADDR, 192.23.40.1),
(IP_DST_ADDR, 210.20.20.6),
(TCP_DST_PORT, HTTP)
```

in cui:

la prima coppia (ETH\_PROT, IP) indica che il protocollo contenuto nel livello Ethernet deve essere il protocollo IP;

la seconda coppia (IP\_SRC\_ADDR, 192.23.40.1) indica che l'indirizzo IP di chi invia il pacchetto deve essere quello indicato;

la terza coppia (IP\_DST\_ADDR, 210.20.20.6) indica che l'indirizzo IP di chi riceve il pacchetto deve essere quello indicato; e

la quarta coppia (TCP\_DST\_PORT, HTTP) indica che il servizio TCP utilizzato è quello HTTP (web).

Gli identificativi posti a destra delle coppie possono assumere anche valori non definiti a priori, ad esempio nel caso in cui si vogliano identificare tutti gli indirizzi di una sottorete. In tal caso l'indirizzo dell'esempio precedente può essere espresso come 210.20.20.\* dove il simbolo \* (asterisco) indica un valore jolly, vale a dire tutti i possibili valori che possono essere presenti in quella posizione. Nell'ambito della stessa coppia possono apparire due o più asterischi: ad esempio

210.\*.20.\* indicando così un insieme di 65536 (o più) indirizzi diversi. Altre forme accettate sono ad esempio: 2\*.20.20.\* indicando tutti gli indirizzi che iniziano con 2 e terminano con un sottoindirizzo tra 0 e 255 (in totale in questo caso  $100 \times 256 = 25600$  indirizzi diversi).

Un ulteriore esempio di pattern per il riconoscimento del protocollo IBM NetBios tra due elaboratori è il seguente:

```
(ETH_PROT, IEEE802),
(IEEE802_DST_SAP, IBM_NETBIOS)
```

Volendo inoltre forzare anche il riconoscimento delle schede di rete (sono 6 bytes che includono il codice costruttore della scheda ed il numero della scheda) coinvolte nella comunicazione NetBios, il pattern diventa:

```
(ETH_SRC_ADDR, 0xFF45DE782201),
(ETH_DST_ADDR, 0xF237C811000F),
(ETH_PROT, IEEE802),
(IEEE802_DST_SAP, IBM_NETBIOS).
```

*Elemento 202:*

E' il compilatore di pattern ed è composto da un elemento di conversione delle regole contenute in 201 in un insieme di sequenze di identificatori numerici e da un elemento di compressione degli identificatori

così ottenuti.

i) Elemento di conversione

Le regole di riconoscimento che si presentano quali coppie <tipo di dato>/<valore dato> vengono convertite in sequenze di identificatori numerici che costituiscono la base di riconoscimento delle trame lette da rete.

Data ad esempio la regola

```
(ETH_PROT, IP),
(IP_SRC_ADDR, 228.186.33.90),
(IP_DST_ADDR, 41.240.227.149),
(TCP_DST_PORT, HTTP)
```

abbiamo che:

a) la prima coppia (ETH\_PROT, IP) viene convertita in due coppie di dati in esadecimale (in cui il prefisso 0x indica che il valore successivo è rappresentato in esadecimale):

0x0C 0x0800

0x49 0x06

in cui:

- la prima riga contiene due valori, 0C e 0800. La cifra più a sinistra del primo valore (0) indica che si è in presenza di una trama Ethernet. La seconda cifra del primo valore (C) indica la posizione all'interno della trama (13° byte, considerando il

primo in posizione 0). Il secondo valore (0800) è il codice identificativo del protocollo IP quando contenuto in una trama Ethernet; e

- la seconda riga contiene due valori, 49 e 06. La cifra più a sinistra del primo valore (4) indica che si è in presenza di una trama IP. La seconda cifra del primo valore (9) indica la posizione all'interno della trama. Il secondo valore (06) è identificativo del protocollo TCP contenuto in IP.

b) la seconda coppia (IP\_SRC\_ADDR, 228.186.33.90) viene convertita in quattro coppie di dati in esadecimale:

0x4C 0xe4

0x4D 0xba

0x4E 0x21

0x4F 0x5a

in cui ciascuna coppia indica rispettivamente la trama IP (4), la posizione (da C ad F) ed il valore di ogni singolo elemento che costituisce l'indirizzo del trasmettitore (source address): e4 in esadecimale corrisponde infatti a 228 in decimale, ba in esadecimale corrisponde a 186 in decimale, 21 in esadecimale corrisponde a 33 in decimale e 5a in esadecimale corrisponde a 90 in decimale.

c) la terza coppia (IP\_DST\_ADDR, 41.240.227.149)



```
(IP_SRC_ADDR, 228.186.33.90),
(IP_DST_ADDR, 41.240.227.149),
(TCP_DST_PORT, HTTP)
```

si ottiene la sequenza

```
0x0C 0x0800, 0x49 0x06, 0x4C 0xe4, 0x4D 0xba, 0x4E
0x21, 0x4F 0x5a, 0x410 0x29, 0x411 0xf0, 0x412 0xe3,
0x413 0x95, 0x82 0x0080.
```

E' da intendersi che tutte le conversioni fin qui descritte sono rese possibili tramite un confronto sequenziale di ciascuna delle coppie <tipo di dato>/<valore dato> con una tabella memorizzante tutte le possibili coppie <tipo di dato>/<valore dato> unitamente alla corrispondente coppia di valori esadecimali.

In realtà per le regole così definite può utilizzarsi un formalismo più esteso, semanticamente rappresentabile dalla coppia <oggetto>/<azione>. Il campo <oggetto> indica l'insieme di proprietà (compreso il valore) assunte dall'elemento correntemente sotto esame, mentre il campo <azione> esprime le azioni da eseguire dopo aver riconosciuto tale oggetto nella trama di comunicazione.

Nelle coppie esadecimali del tipo <tipo di dato>/<valore dato> è ad esempio facile notare come il campo <tipo di dato> contenga una doppia informazione,

vale a dire sia il protocollo (o il tipo di trama) cui si fa riferimento, sia anche la posizione all'interno di tale protocollo.

Nel caso di protocolli applicativi complessi, le trame rilevate vengono in genere rappresentate tramite un linguaggio di tipo LL(1) (vale a dire, secondo la definizione di Chomsky, un linguaggio che non presenta strutture di controllo e che non presenta limiti per la definizione dei meccanismi di interpretazione delle strutture informative). In tale caso il campo <azione> farà riferimento ad un insieme minimo di comandi elementari, qui riportati:

- Push

<valore>

<variabile>

<posizione di lettura>

<valore alla posizione di lettura>

- Pop

<variabile>

<posizione di lettura>

<nella posizione di lettura>

- And

- Mul

- Add

- Equal

- Next
- F\_send\_all
- F\_dynamic

Qui di seguito viene fornito, a scopo di completezza, un breve cenno al significato di tali comandi elementari.

- Push <valore> inserisce un valore nello stack riservato al processo di riconoscimento in atto, ad esempio: PUSH(35), il valore 35 viene messo nello stack;

- Push <variabile> inserisce il contenuto di una variabile nello stack riservato al processo di riconoscimento in atto, ad esempio: PUSH(v12), se la variabile "v12" vale 8, 8 viene messo nello stack;

- Push <posizione di lettura> inserisce nello stack riservato al processo di riconoscimento in atto la posizione del valore correntemente da leggere nello stream di input, ad esempio PUSH(pos) se pos, variabile che indica la posizione di lettura, vale 5, allora 5 viene messo nello stack;

- Push <valore alla posizione di lettura> inserisce nello stack riservato al processo di riconoscimento in atto il valore letto nello stream di input in fase di riconoscimento al posto "posizione di lettura", ad



esempio PUSH(v\_pos), se pos, variabile che indica la posizione di lettura, vale 5 e se al posto 5 dello stream di input c'è il valore 30, allora 30 viene messo nello stack;

- Pop <variabile> inserisce la testa dello stack nella variabile "variabile", ad esempio POP(v3) ,se nella testa dello stack è stato inserito il valore 10, significa che l'ultima operazione fatta con lo stack è stata ad esempio push(10), il valore 10 va nella variabile "v3";

- Pop <posizione di lettura> inserisce la testa dello stack nella variabile che indica la prossima posizione da leggere nello stream di input, ad esempio POP(pos) ,se nella testa dello stack è stato inserito il valore 10, il prossimo elemento che verrà letto dallo stream di input sarà quello in posizione 10;

- Pop <nella posizione di lettura> inserisce la testa dello stack nella posizione indicata dalla variabile che indica la prossima posizione da leggere nello stream di input, ad esempio POP(v\_pos) ,se nella testa dello stack è stato inserito il valore 10, il prossimo elemento che verrà letto dallo stream di input avrà valore 10;

- And, Mul, Add, Or, Sub sono tutte operazioni aritmetiche e logiche. L'operazione viene svolta sui

valori contenuti nelle prime due posizione dello stack, il risultato diventa la testa dello stack e i due valori utilizzati sono tolti dallo stack; esempio: le operazioni logico aritmetiche seguono la notazione polacca inversa (RPN). Supponiamo di dover eseguire l'operazione  $10 \times 30$ : il programma che ne consegue avrà la seguente forma:

PUSH(10)

PUSH(30)

MUL

ora, nella testa dello stack c'è  $300 = 30 \times 10$ .

- Equal <valore>, Equal <variabile>, Equal <posizione di lettura>, Equal <valore nella posizione di lettura> verifica se nella testa dello stack c'è un valore uguale a quello passato come parametro. Il risultato (0 se diversi, 1 se uguali) viene messo nella testa dello stack;

- f\_send\_all è una funzione che, quando eseguita, riporta verso l'output l'intero stream di input;

- Next <valore>, Next <variabile> incrementa di "valore" oppure del valore contenuto nella "variabile" la variabile che indica la posizione nello stream di input dove leggere il prossimo valore; ed infine

- f\_dynamic("nome") esegue la funzione "nome" collegata all'elemento di coordinamento attraverso

meccanismi di collegamento dinamico (tipo DLL di windows oppure shared\_libraries di UNIX oppure meccanismi RPC di DCE, ...) passandogli come parametri i valori contenuti nello stack.

Una possibile sintassi implementativa (ripresa dal linguaggio C) dell'insieme delle coppie <oggetto>/<azione> potrà essere la seguente:

```
typedef struct _item {
    unsigned char oggetto;
    unsigned long int azione;
} Item;
```

```
typedef struct _record {
    int num_of_items;
    Item * items;
} Record;
```

```
Record * input_seconda_fase;
```

in cui:

- il campo "oggetto" è stato espresso come un singolo byte ("unsigned char"). Una tale scelta non comporta limitazioni in quanto un valore intero (lungo da 2 a 4 byte) può essere considerato come una sequenza di byte e quindi può essere trattato un byte alla volta; e

- il campo "azione" è stato espresso come "unsigned long int". Può quindi rappresentare sia un numero (compatibile con la prima notazione) sia come puntatore ad una struttura o insieme di funzioni (compatibile con la seconda notazione).

Il numero di sequenze diverse è in genere molto elevato. A titolo di esempio, considerando esclusivamente il protocollo TCP-IP, per un numero relativamente esiguo di 1000 "clients" (cioè di elaboratori che utilizzano servizi applicativi resi disponibili da altri elaboratori) e di 10 "servers" (cioè di elaboratori che forniscono i servizi applicativi ai clients) e di una media di 10 servizi applicativi per "server" (quali ad esempio FTP, TELNET, HTTP, MAIL, NFS, TIME, DNS), al fine di distinguere tutti i possibili "accoppiamenti" tra client-server-servizio, è necessario definire regole atte ad indicare  $1000 \cdot 10 \cdot 10 = 100000$  sequenze diverse di pattern nelle trame di comunicazione.

Questo numero, già ben al di sopra delle dimensioni ritenute accettabili per le tavole interne di indirizzamento dei router e dei firewall commerciali, cresce in modo molto rapido quando si vanno a definire regole che agiscono non solo a livello di parte di controllo dei protocolli di



comunicazione ma anche a livello di parte dati, secondo quanto accade nella presente invenzione.

Il linguaggio delle regole sopra definito consente di redigere regole che permettono di identificare elementi della parte dati del protocollo di comunicazione: se si vuole infatti non soltanto "identificare" un "client" ma anche quando questo su rete cerca di accedere ad una particolare pagina WEB (cosa del tutto possibile tramite la presente invenzione), non è sufficiente agire a livello di parte di controllo del protocollo di comunicazione (si riuscirebbe a riconoscere solo il fatto che è stato inviato un comando a livello di servizio HTTP) ma è necessario agire a livello di parte dati del protocollo TCP-IP al fine di identificare la particolare stringa che determina l'accesso alla pagina WEB richiesta dal client.

ii) Elemento di compressione dell'insieme di sequenze ottenute in una struttura dati ad accesso diretto

Tale secondo elemento del compilatore di pattern 202 permette una costruzione della struttura dati di compressione che è in grado di garantire un tempo di accesso costante (indipendente cioè dalla numerosità delle sequenze) ed un'occupazione di memoria ottimale

(pari cioè, a meno di una costante moltiplicativa, alla quantità di memoria necessaria per memorizzare le sequenze in modo non strutturato) per il riconoscimento delle sequenze memorizzate in tale struttura nelle trame di comunicazione che si leggono da rete.

Verrà in particolare fatto riferimento agli articoli:

- a) "Time Optimal Digraph Browsing on a Sparse Representation", Tech. Report, Dipartimento di Matematica, Università di Roma "Tor Vergata", 8/97, 1997 di M. Talamo e P. Vocca;
- b) "Optimal Bounds on Complexity of Sparse Partial Orders", Tech. Report Dipartimento di Matematica, Università di Roma "Tor Vergata", 9/97, 1997 di M. Talamo e P. Vocca;
- c) "Optimal Digraph Search on a Compressed Representation", Tech. Report Dipartimento di Matematica, Università di Roma "Tor Vergata", 11/98, 1998 di M. Talamo e P. Vocca; e
- d) "Compact Implicit Representation of Graphs", proceedings WG98, giugno 1998 di M. Talamo e P. Vocca.

In tali scritti si rappresentano strutture dati che permettono una accessibilità a tempo costante, vale a dire indipendente dalla numerosità di dati che

queste rappresentano.

L'algoritmo per l'ottenimento di tali strutture di dati si applica a strutture di ingresso del tipo a "grafo bipartito", come ad esempio rappresentato in figura 10A. In tale grafo i nodi possono essere distinti in due sottoinsiemi distinti (da A ad E e da 0 a 4 in figura), in maniera tale che ciascun nodo appartenente ad un primo sottoinsieme possa essere connesso solamente a nodi appartenenti al secondo sottoinsieme e viceversa. Con riferimento alla figura 10A, il nodo A è connesso al nodo 0 ed al nodo 2, il nodo B è connesso al nodo 0 ed al nodo 2, il nodo C è connesso al nodo 1 ed al nodo 4, il nodo D è connesso al nodo 3 ed il nodo E è connesso al nodo 3.

Tali connessioni possono essere espresse mediante una matrice bidimensionale del tipo riportato in figura 10B, ove con il simbolo x sono state riportate le connessioni attive tra righe e colonne. Si può pertanto concludere che i grafi bipartiti sono equivalenti alle matrici bidimensionali e che pertanto i risultati di accessibilità a tempo costante ottenuti con riferimento all'articolo sopra citato possono applicarsi anche a strutture quali matrici bidimensionali.

L'elemento di compressione sarà pertanto tale da

comprimere le sequenze ottenute tramite l'elemento di conversione e da generare una molteplicità di matrici bidimensionali indicative di tali sequenze.

\* \* \*

L'algoritmo tramite il quale l'elemento di compressione opera, qui di seguito presentato, (da PASSO 1 a PASSO 11) è da intendersi implementato in un qualsiasi linguaggio di programmazione adatto allo scopo (ad esempio in linguaggio C) e memorizzato all'interno di una ROM.

L'input dell'algoritmo consiste nella sequenza di identificativi numerici (record) a lunghezza variabile precedentemente specificata.

Congiuntamente ai vari passi dell'algoritmo, si riporterà a livello esemplificativo un ciclo completo di compilazione per un particolare caso pratico, al fine di descrivere in maniera compiuta le modalità operative dell'algoritmo stesso. A scopo esemplificativo si continuerà a fare riferimento a strutture di comunicazione del tipo Ethernet. E' da intendersi che il funzionamento del dispositivo di controllo secondo la presente invenzione resta inalterato anche nel caso in cui l'apparecchio di rilevamento ed interpretazione non fornisca trame Ethernet rilevate sulla rete ma fornisca direttamente



comunicazioni a livello TCP/IP o comunque stream di dati anche molto lunghi.

PASSO 1 (specifica regole predefinite, si veda anche la figura 11):

Si supponga di dover gestire e coordinare trame di comunicazione a livello Ethernet tramite i seguenti schemi di connettività:

connessione a) 132.147.200.10 potrà connettersi a 132.147.160.1 solamente per il servizio:

- WWW servizio TCP 80.

connessione b) 132.147.200.10 potrà connettersi a 132.147.160.2 solamente per i servizi:

- SMTP servizio TCP 25;
- NETBIOS servizi TCP 137, 138 e 139.

connessione c) 132.147.200.20 potrà connettersi a 132.147.160.1 solamente per i servizi:

- FTP servizio TCP 20 e 21;
- TELNET servizio TCP 23.

connessione d) 132.147.200.20 potrà connettersi a 132.147.160.2 solamente per i servizi:

- SMTP servizio TCP 25;
- WWW servizio TCP 80.

connessione e) 132.147.200.20 potrà connettersi a 132.147.160.3 solamente per i servizi:

- WWW servizio TCP 80;

- SNMP servizi TCP 161 e 162;
- NFS servizio TCP 2049;
- TELNET servizio TCP 23.

Inoltre dovranno essere ammesse tutte le comunicazioni di tipo ARP (protocollo a livello Ethernet) e ICMP (protocollo a livello IP).

PASSO 2 (conversione regole in un insieme di sequenze):

In base a tale schema di connessione si ottiene un insieme di 17 record (in cui ogni record è formato da un insieme di coppie <oggetto>/<azione>). In particolare, il record 1 rappresenta la connessione a), i record da 2 a 5 rappresentano la connessione b), i record da 6 a 8 rappresentano la connessione c), i record da 9 a 10 rappresentano la connessione d), i record da 11 a 15 rappresentano la connessione e), il record 16 rappresenta il protocollo ARP in Ethernet ed infine il record 17 rappresenta il protocollo ICMP in IP.

Connessione a)

RECORD 1

0x08, 0x000C

0x00, 0x000D

protocollo IP in Ethernet

0x06, 0x4009	protocollo TCP in IP
0x84, 0x400C	
0x93, 0x400D	
0xC8, 0x400E	
0x0A, 0x400F	132.147.200.10
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	
0x01, 0x4013	132.147.160.1
0x00, 0x8002	
0x50, 0x8003	WWW 80

Connessione b)

RECORD 2

0x08, 0x000C	
0x00, 0x000D	protocollo IP in Ethernet
0x06, 0x4009	protocollo TCP in IP
0x84, 0x400C	
0x93, 0x400D	
0xC8, 0x400E	
0x0A, 0x400F	132.147.200.10
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	
0x02, 0x4013	132.147.160.2

0x00, 0x8002

0x19, 0x8003

SMTP 25

RECORD 3

0x08, 0x000C

0x00, 0x000D

protocollo IP in Ethernet

0x06, 0x4009

protocollo TCP in IP

0x84, 0x400C

0x93, 0x400D

0xC8, 0x400E

0x0A, 0x400F

132.147.200.10

0x84, 0x4010

0x93, 0x4011

0xA0, 0x4012

0x02, 0x4013

132.147.160.2

0x00, 0x8002

0x89, 0x8003

NETBIOS 137



RECORD 4

0x08, 0x000C

0x00, 0x000D

protocollo IP in Ethernet

0x06, 0x4009

protocollo TCP in IP

0x84, 0x400C

0x93, 0x400D

0xC8, 0x400E

0x0A, 0x400F	132.147.200.10
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	
0x02, 0x4013	132.147.160.2
0x00, 0x8002	
0x8A, 0x8003	NETBIOS 138

RECORD 5

0x08, 0x000C	
0x00, 0x000D	protocollo IP in Ethernet
0x06, 0x4009	protocollo TCP in IP
0x84, 0x400C	
0x93, 0x400D	
0xC8, 0x400E	
0x0A, 0x400F	132.147.200.10
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	
0x02, 0x4013	132.147.160.2
0x00, 0x8002	
0x8B, 0x8003	NETBIOS 139

Connessione c)

RECORD 6

0x08, 0x000C	
0x00, 0x000D	protocollo IP in Ethernet
0x06, 0x4009	protocollo TCP in IP
0x84, 0x400C	
0x93, 0x400D	
0xC8, 0x400E	
0x14, 0x400F	132.147.200.20
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	
0x01, 0x4013	132.147.160.1
0x00, 0x8002	
0x14, 0x8003	FTP 20

RECORD 7

0x08, 0x000C	
0x00, 0x000D	protocollo IP in Ethernet
0x06, 0x4009	protocollo TCP in IP
0x84, 0x400C	
0x93, 0x400D	
0xC8, 0x400E	
0x14, 0x400F	132.147.200.20
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	

0x01, 0x4013	132.147.160.1
0x00, 0x8002	
0x15, 0x8003	FTP 21

RECORD 8

0x08, 0x000C	
0x00, 0x000D	protocollo IP in Ethernet
0x06, 0x4009	protocollo TCP in IP
0x84, 0x400C	
0x93, 0x400D	
0xC8, 0x400E	
0x14, 0x400F	132.147.200.20
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	
0x01, 0x4013	132.147.160.1
0x00, 0x8002	
0x17, 0x8003	TELNET 23

Connessione d)

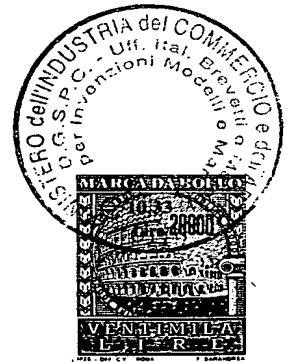
RECORD 9

0x08, 0x000C	
0x00, 0x000D	protocollo IP in Ethernet
0x06, 0x4009	protocollo TCP in IP
0x84, 0x400C	

0x93, 0x400D	
0xC8, 0x400E	
0x14, 0x400F	132.147.200.20
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	
0x02, 0x4013	132.147.160.2
0x00, 0x8002	
0x19, 0x8003	SMTP 25

RECORD 10

0x08, 0x000C	
0x00, 0x000D	protocollo IP in Ethernet
0x06, 0x4009	protocollo TCP in IP
0x84, 0x400C	
0x93, 0x400D	
0xC8, 0x400E	
0x14, 0x400F	132.147.200.20
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	
0x02, 0x4013	132.147.160.2
0x00, 0x8002	
0x50, 0x8003	WWW 80



Connessione e)

RECORD 11

0x08, 0x000C	
0x00, 0x000D	protocollo IP in Ethernet
0x06, 0x4009	protocollo TCP in IP
0x84, 0x400C	
0x93, 0x400D	
0xC8, 0x400E	
0x14, 0x400F	132.147.200.20
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	
0x03, 0x4013	132.147.160.3
0x00, 0x8002	
0x50, 0x8003	WWW 80

RECORD 12

0x08, 0x000C	
0x00, 0x000D	protocollo IP in Ethernet
0x06, 0x4009	protocollo TCP in IP
0x84, 0x400C	
0x93, 0x400D	
0xC8, 0x400E	
0x14, 0x400F	132.147.200.20
0x84, 0x4010	

0x93, 0x4011	
0xA0, 0x4012	
0x03, 0x4013	132.147.160.3
0x00, 0x8002	
0xA1, 0x8003	SNMP 161

RECORD 13

0x08, 0x000C	
0x00, 0x000D	protocollo IP in Ethernet
0x06, 0x4009	protocollo TCP in IP
0x84, 0x400C	
0x93, 0x400D	
0xC8, 0x400E	
0x14, 0x400F	132.147.200.20
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	
0x03, 0x4013	132.147.160.3
0x00, 0x8002	
0xA2, 0x8003	SNMP 162

RECORD 14

0x08, 0x000C	
0x00, 0x000D	protocollo IP in Ethernet
0x06, 0x4009	protocollo TCP in IP

0x84, 0x400C	
0x93, 0x400D	
0xC8, 0x400E	
0x14, 0x400F	132.147.200.20
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	
0x03, 0x4013	132.147.160.3
0x08, 0x8002	
0x01, 0x8003	NFS 2049

RECORD 15

0x08, 0x000C	
0x00, 0x000D	protocollo IP in Ethernet
0x06, 0x4009	protocollo TCP in IP
0x84, 0x400C	
0x93, 0x400D	
0xC8, 0x400E	
0x14, 0x400F	132.147.200.20
0x84, 0x4010	
0x93, 0x4011	
0xA0, 0x4012	
0x03, 0x4013	132.147.160.3
0x00, 0x8002	
0x17, 0x8003	TELNET 23

ed infine

RECORD 16

0x08, 0x000C

0x06, 0x000D                      protocollo ARP in Ethernet

RECORD 17

0x08, 0x000C

0x00, 0x000D                      protocollo IP in Ethernet

0x01, 0x4009                      protocollo ICMP in IP

La struttura così ottenuta può essere espressa in forma matriciale, secondo la rappresentazione di figura 12. Si noti come i vari record possono avere lunghezze diverse. Si hanno infatti 15 record di lunghezza 13, 1 record di lunghezza 2 ed 1 record di lunghezza 3.

PASSO 3:

Si pone  $CONT = 0$

PASSO 4:

Si prende la colonna 0 e la colonna CONT della sequenza sopra riportata e si costruisce una nuova sequenza di record che contengono solo 2 item (quello in colonna 0 e quello in colonna CONT).



PASSO 5:

Da questa nuova sequenza di record si eliminano i duplicati.

PASSO 6:

Si pone  $RIGA=0$

PASSO 7:

Con la nuova sequenza di record si costruisce un grafo bipartito pesato inserendo per ogni record:

- il valore dell'item in posizione 0 (id del nodo superiore);
- il valore dell'item in posizione CONT (id del nodo inferiore);
- l'azione dell'item in posizione CONT (quale primo peso dell'arco tra i due nodi);
- RIGA (quale secondo peso dell'arco tra i due nodi).

Inoltre, per ogni coppia di nodi inserita, si sostituisce al valore dell'item in posizione 0 nella sequenza di record originale il nuovo valore RIGA e si pone  $RIGA=RIGA+1$ .

PASSO 8:

Si converte il grafo bipartito così ottenuto in una

matrice bidimensionale ed in un vettore tramite utilizzo dell'algoritmo di base di cui alle pubblicazioni sopra menzionate. Si noti comunque che l'algoritmo qui descritto costituisce un'estensione di tale algoritmo di base, in particolare per quanto riguarda il precedente passo 7.

PASSO 9:

Si memorizzano la matrice bidimensionale ed il vettore.

PASSO 10:

Si pone  $CONT=CONT+1$

PASSO 11:

Se  $CONT$  non è pari al numero massimo di item dei record, si torna al passo 4, altrimenti l'algoritmo è terminato.

\* \* \*

La sequenza di matrici bidimensionali e vettori costituisce la struttura dati compressa che sarà utilizzata per il riconoscimento degli stream di ingresso. Tale struttura è accessibile in maniera diretta.

Si farà d'ora in poi nuovamente riferimento alla

figura 9.

*Elemento 203* (Memoria contenente i pattern compressi):

Tale elemento è costituito dalla sequenza di matrici ottenute come risultato dell'algoritmo di compressione di cui sopra. Grazie all'elevato grado di compressione di tale algoritmo, la dimensione di questa sequenza di matrici è direttamente proporzionale al numero di connessioni attive della matrice originale e quindi è direttamente memorizzabile in memoria centrale. In caso di elevata numerosità di connessioni attive ( $>100.000.000$ ) è possibile gestire tale sequenza di matrici compresse tramite dispositivi di memoria di massa.

*Elemento 204* (Riconoscitore dei pattern):

Tale elemento permette il confronto tra le trame applicative da riconoscere rilevate tramite l'elemento 205 e la struttura dati ad accesso diretto memorizzata in 203.

L'elemento 204 è realizzato in un microchip ed è sostanzialmente costituito da un software che implementa una tecnica di accesso diretto su matrici, al fine di accedere alle matrici memorizzate in 203.

Si è pertanto in grado di riconoscere in modo completamente deterministico l'accettabilità o la non accettabilità della trama letta da rete.

\* \* \*

Al fine di fornire un esempio dettagliato del funzionamento di tale riconoscitore, viene qui di seguito innanzitutto riportata la struttura delle matrici memorizzate in 203, tramite utilizzo di una sintassi simile a quella del linguaggio C:

//Struttura per una Matrice bidimensionale ed un vettore

```
typedef struct _matrici_AB {
    unsigned long int row_a; //Numero di righe della
    matrice
    unsigned long int col_a; //Numero di colonne
    della matrice
    unsigned long int col_b; //Numero di elementi
    del vettore
    unsigned long int **mA; //Matrice dei valori
    Azione ***mP; //Matrice delle Azioni
    unsigned long int *mB; //Vettore
} mat_AB;
```

```
typedef struct _vec_matrici_AB {
    mat_AB * MAB; //Insieme delle matrici e
    dei vettori
    unsigned long int num_mab; //Numero delle matrici
    e dei vettori
```



S.I.B.  
ROMA

```
} * Vec_mat_AB;
```

Si riportano poi qui di seguito cinque record di ingresso e le matrici risultanti. In tale esempio la descrizione dei record viene fatta tramite la sintassi <oggetto>/<azione> precedentemente riportata. Le azioni associate sono estremamente semplificate (una sola azione per ogni riconoscimento). Per semplicità si suppone inoltre che il riconoscimento inizi sempre dal primo byte dello stream in ingresso.

#### RECORD 1

```
0x01 next(1)
```

```
0x03 next(1)
```

```
0x02 f_send_all
```

#### RECORD 2

```
0x01 next(1)
```

```
0x06 next(1)
```

```
0x04 f_send_all
```

#### RECORD 3

```
0x02 next(1)
```

```
0x07 next(1)
```

```
0x03 f_send_all
```

#### RECORD 4

```
0x01 next(1)
```

0x02 f\_send\_all

RECORD 5

0x05 next(1)

0x01 f\_send\_all

Per next(1) si intende l'azione di posizionamento sul prossimo byte nello stream di dati. Per f\_send\_all si intende l'azione di inoltro verso l'esterno di tutto lo stream di dati.

Tramite l'algoritmo precedentemente descritto si viene ad ottenere la seguente struttura matriciale:

1	MATRICE DEI VALORI  0: [ X ] 1: [ 0 ] 2: [ 1 ] 3: [ X ] 4: [ X ] 5: [ 2 ]	MATRICE DELLE AZIONI  (1, 0) NEXT(1) (2, 0) NEXT(1) (5, 0) NEXT(1)	VETTORE B  X 0 0 X X 0
2	MATRICE DEI VALORI  0: [ X ]	MATRICE DELLE AZIONI  (1, 0)	VETTORE B  0 0 0

	1: [ 4 ]	F_SEND_ALL	
	2: [ 0 ]	(2, 0)	
	3: [ 1 ]	F_SEND_ALL	
	4: [ X ]	(3, 0) NEXT(1)	
	5: [ X ]	(6, 0) NEXT(1)	
	6: [ 2 ]	(7, 0) NEXT(1)	
	7: [ 3 ]		
3	MATRICE DEI VALORI	MATRICE DELLE AZIONI	VETTORE B
	0: [0 4 ]	(2, 0)	0 0 0 0 1
	1: [X X ]	F_SEND_ALL	
	2: [1 X ]	(3, 0)	
	3: [3 X ]	F_SEND_ALL	
	4: [2 X ]	(4, 0)	
		F_SEND_ALL	

Per non appesantire la presente descrizione non verranno qui descritte nel dettaglio le varie operazioni (in fondo semplici applicazioni dell'algoritmo sopra descritto) che portano dai record alla struttura matriciale ora graficata. A scopo di chiarezza, la matrice dei valori è stata poi rappresentata fisicamente separata dalla matrice delle

azioni.

Verranno invece descritte in dettaglio le operazioni di confronto che vengono eseguite al fine di riconoscere o meno gli stream di dati rilevati. Tali operazioni si riferiscono al caso particolare della struttura matriciale di cui sopra.

1) ESEMPIO DI RICONOSCIMENTO NEL CASO IN CUI LO STREAM SIA IDENTICO AL RECORD 1: 0x01 0x03 0x02

Il primo valore letto è 01.

Essendo nella condizione iniziale lo si usa sia come indice della matrice che del vettore.

La coppia Matrice/Vettore che si utilizza è nella posizione 1 dell'elenco sopra riportato.

L'indice di riga della matrice A viene determinato dall'elemento letto, vale a dire Riga A = 01, cioè la prima riga.

L'indice di colonna della matrice A viene determinato dal valore contenuto dal vettore B nella posizione corrispondente all'elemento letto, vale a dire Colonna A = B[0x01]=0, cioè la zeresima colonna.

Si andrà pertanto a leggere il valore riportato in A[1, 0] e cioè 0. Tale valore costituisce il prossimo indice del vettore B.

Si andrà poi a leggere l'azione riportata in A[1, 0] vale a dire il valore numerico corrispondente



all'azione next(1).

Verrà pertanto eseguita la suddetta azione e dunque ci si posizionerà sul prossimo valore dello stream di dati.

Si andrà al prossimo valore e si utilizzerà quindi la coppia Matrice/Vettore che è nella posizione 2 dell'elenco sopra riportato.

Il valore letto è 03.

L'indice di riga della matrice A viene determinato dall'elemento letto, vale a dire Riga A = 03, cioè la terza riga.

L'indice di colonna della matrice A viene determinato dal valore contenuto dal vettore B nella posizione corrispondente al valore riportato in A[1, 0] ottenuto nel passo precedente (e cioè 0). Colonna A = B[0] = 0, cioè la zeresima colonna.

Si andrà pertanto a leggere il valore riportato in A[3, 0] e cioè 1. Tale valore costituisce il prossimo indice del vettore B.

Si andrà poi a leggere l'azione riportata in A[3, 0] vale a dire il valore numerico corrispondente all'azione next(1).

Verrà pertanto eseguita la suddetta azione e dunque ci si posizionerà sul prossimo valore dello stream di dati.

Si andrà al prossimo valore e si utilizzerà quindi la coppia Matrice/Vettore che è nella posizione 3 dell'elenco sopra riportato.

Il valore letto è 02.

L'indice di riga della matrice A viene determinato dall'elemento letto, vale a dire Riga A = 02, cioè la seconda riga.

L'indice di colonna della matrice A viene determinato dal valore contenuto dal vettore B nella posizione corrispondente al valore riportato in A[3, 0] ottenuto nel passo precedente (e cioè 1). Colonna A = B[1] = 0, cioè la zerosima colonna.

Si andrà pertanto a leggere il valore riportato in A[2, 0] e cioè 1. Tale valore costituisce il prossimo indice del vettore B.

Si andrà poi a leggere l'azione riportata in A[2, 0] vale a dire il valore numerico corrispondente all'azione `f_send_all`. Ciò significa che è avvenuto il riconoscimento.

2) ESEMPIO DI RICONOSCIMENTO NEL CASO IN CUI LO STREAM SIA DIVERSO DAI RECORD: 0x04 0x01

Il primo valore letto è 04.

Essendo nella condizione iniziale lo si usa sia come indice della matrice che del vettore.

La coppia Matrice/Vettore che si utilizza è nella

posizione 1 dell'elenco sopra riportato.

L'indice di riga della matrice A viene determinato dall'elemento letto, vale a dire Riga A = 04, cioè la quarta riga.

L'indice di colonna della matrice A viene determinato dal valore contenuto dal vettore B nella posizione corrispondente all'elemento letto, vale a dire Colonna A = B[04] = X. Lo stream non viene pertanto riconosciuto.

3) ESEMPIO DI RICONOSCIMENTO NEL CASO IN CUI LO STREAM SIA DIVERSO DAI RECORD: 0x01 0x05 0x03

Il primo valore letto è 01.

Essendo nella condizione iniziale lo si usa sia come indice della matrice che del vettore.

La coppia Matrice/Vettore che si utilizza è nella posizione 1 dell'elenco sopra riportato.

L'indice di riga della matrice A viene determinato dall'elemento letto, vale a dire Riga A = 01, cioè la prima riga.

L'indice di colonna della matrice A viene determinato dal valore contenuto dal vettore B nella posizione corrispondente all'elemento letto, vale a dire Colonna A = B[0x01] = 0, cioè la zeresima colonna.

Si andrà pertanto a leggere il valore riportato in A[1, 0] e cioè 0. Tale valore costituisce il

prossimo indice del vettore B.

Si andrà poi a leggere l'azione riportata in  $A[1, 0]$  vale a dire il valore numerico corrispondente all'azione  $next(1)$ .

Si andrà pertanto al prossimo valore e si utilizzerà quindi la coppia Matrice/Vettore che è nella posizione 2 dell'elenco sopra riportato.

Il valore letto è 05.

L'indice di riga della matrice A viene determinato dall'elemento letto, vale a dire Riga A = 05, cioè la quinta riga.

L'indice di colonna della matrice A viene determinato dal valore contenuto dal vettore B nella posizione corrispondente al valore riportato in  $A[1, 0]$  ottenuto nel passo precedente. Colonna A =  $B[0] = 0$ .

Bisognerà pertanto andare a leggere il valore riportato in  $A[5, 0]$  e cioè X. Lo stream non viene pertanto riconosciuto.

Il riconoscitore di pattern, quindi, usando una tecnica ad accesso diretto su matrici, facilmente implementabile in un microchip è in grado di riconoscere in modo completamente deterministico l'accettabilità o la non accettabilità dello stream in ingresso in un numero di accessi a matrici e vettori, pari al numero degli elementi riconosciuti nello



stream stesso

\* \* \*

Si farà d'ora in poi nuovamente riferimento alla figura 9.

*Elemento 205:*

E' la componente di rilevamento ed acquisizione delle trame di comunicazione. Tramite questo apparecchio, un esempio del quale è già stato descritto in dettaglio con riferimento alle precedenti figure da 4 ad 8B, viene resa possibile l'acquisizione di dati anche a livello applicativo, vale a dire l'informazione relativa ai livelli 4-7 dello standard OSI. Tale apparecchio potrà accettare comandi quali i comandi CONNECT, SEND, RECEIVE e CLOSE nel caso in cui si debbano gestire e coordinare protocolli applicativi di alto livello.

*Elemento 206 (Controllo accessi):*

Questo elemento, a partire dal risultato di riconoscimento operato dall'elemento 204, esegue l'azione di inoltro associata a tale riconoscimento oppure l'azione di rifiuto associata al non riconoscimento.

Nel caso di accettazione la trama di comunicazione verrà inoltrata al server di riferimento.

Nel caso di rifiuto, la trama di comunicazione verrà rispedita al mittente, unitamente alle eventuali motivazioni del rifiuto. Infatti, grazie alla struttura <oggetto>/<azione> adottata, sarà possibile associare azioni, anche complesse, quali la costruzione di stream di risposta.

*Elemento 207 (Coordinamento accessi):*

Questo elemento, a partire dal risultato di riconoscimento operato dall'elemento 204, esegue l'azione di coordinamento associata a tale riconoscimento.

Tale azione di coordinamento riguarda l'individuazione dei parametri da inviare al server per il coordinamento richiesto, l'individuazione del server, la formattazione dei parametri da inviare, l'invio dei parametri, l'acquisizione della risposta dal server e l'inoltro della risposta ottenuta all'elemento 204 per l'eventuale prosecuzione del riconoscimento.

Questo approccio è reso possibile dall'uso della seconda notazione introdotta in quanto grazie a questa notazione è possibile associare azioni, anche complesse, quali la costruzione di stream da inoltrare a particolari server accessibili da rete. L'elemento di coordinamento ha un suo senso compiuto quando si

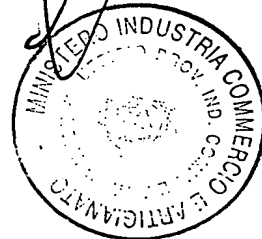
utilizzi lo strumento per la gestione di comunicazioni tra applicazioni e quindi su protocolli ad alto livello (quali quelli tra applicazioni client e server trasportati a livello TCP). In tal caso, infatti, lo strumento, grazie alle azioni associate al riconoscimento degli stream di ingresso, può operare trasformazioni dello stream per il suo reinoltro ad altre applicazioni server che prevedono protocolli applicativi diversi. Un tipico caso è quando si deve gestire l'interoperabilità e la cooperazione applicativa in un contesto eterogeneo e devono coesistere differenti "server applicativi" o differenti dispositivi di mediazione (broker) (facendo in questo caso riferimento anche alle diverse implementazioni di CORBA -Common Object Request Broker Architecture- che non sono mai completamente compatibili tra loro) a fronte di applicazioni utente (client) spesso progettate per dialogare utilizzando protocolli applicativi non aggiornati.

La presente invenzione è stata fin qui descritta con riferimento ad una sua forma di realizzazione illustrata a scopo esemplificativo e non limitativo.

E' da intendersi inoltre che altre siano le forme di realizzazione possibili rientranti nell'ambito della presente privativa industriale.

*Giorgio Strini*  
(Iscr. Albo n. 452 BM)

*Strini*



S.I.B.  
ROMA

RM 98 A 000542

RIVENDICAZIONI

1. Dispositivo di controllo di accessi in rete tramite il riconoscimento deterministico di trame applicative che soddisfano un insieme di regole predefinite comprendente:

- mezzi (205) di rilevamento ed interpretazione delle trame applicative da riconoscere;
- mezzi (201) di memorizzazione di regole predefinite;
- mezzi (202) di compilazione delle regole predefinite in una struttura dati ad accesso diretto;
- mezzi (203) di memorizzazione di detta struttura dati ad accesso diretto; e
- mezzi (204) di confronto tra le trame applicative da riconoscere e detta struttura dati ad accesso diretto, in cui il riconoscimento può essere effettuato su qualsiasi componente della trama ed in cui la struttura dati ad accesso diretto permette di ottenere un tempo di accesso sostanzialmente indipendente dalla numerosità delle regole.

2. Dispositivo di controllo di accessi secondo la rivendicazione 1, caratterizzato dal fatto che detti mezzi (202) di compilazione delle regole predefinite comprendono:

- mezzi di conversione delle regole predefinite in un insieme di sequenze elementari di identificazione

S.I.E.  
ROMA

numerici; e

- mezzi di compressione dell'insieme di sequenze così ottenute in una struttura dati ad accesso diretto.

3. Dispositivo di controllo di accessi secondo la rivendicazione 1 o 2, caratterizzato dal fatto di comprendere inoltre mezzi di inoltro della trama applicativa quando riconosciuta e mezzi di restituzione al mittente della trama applicativa quando non riconosciuta.

4. Dispositivo di controllo di accessi secondo la rivendicazione 3, caratterizzato dal fatto che detti mezzi di restituzione al mittente della trama applicativa quando non riconosciuta prevedono la restituzione di informazioni relative ai motivi del mancato inoltro.

5. Dispositivo di controllo di accessi secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto che le regole predefinite sono memorizzabili quale coppia di campi <oggetto>/<azione>.

6. Dispositivo di controllo di accessi secondo la rivendicazione 5, caratterizzato dal fatto che le regole predefinite sono memorizzate quale coppia di campi <tipo di dato>/<valore dato>.

7. Dispositivo di controllo di accessi secondo la

rivendicazione 5 o la rivendicazione 6, caratterizzato dal fatto che le regole predefinite contengono uno o più valori jolly.

8. Dispositivo di controllo di accessi secondo la rivendicazione 5, caratterizzato dal fatto che il campo <azione> fa riferimento all'insieme minimo di comandi

- Push

<valore>

<variabile>

<posizione di lettura>

<valore alla posizione di lettura>

- Pop

<variabile>

<posizione di lettura>

<nella posizione di lettura>

- And

- Mul

- Add

- Equal

- Next

- F\_send\_all

\* F\_dynamic.

9. Dispositivo di controllo di accessi secondo le rivendicazioni 2 e 5, caratterizzato dal fatto che la

struttura dati ad accesso diretto è rappresentata tramite una struttura matriciale comprendente campi oggetto e campi azione.

10. Dispositivo di controllo di accessi secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto che i mezzi (205) di rilevamento ed interpretazione delle trame applicative comprendono:

- un dispositivo (9) di rilevamento di pacchetti di dati ad un livello corrispondente al livello OSI 2 comprendenti frame di controllo e frame di informazione, in cui i frame di controllo ed informazione comprendono una parte di intestazione ed una parte di corpo, detta parte di intestazione essendo atta a permettere la distinzione tra un frame di informazione ed un frame di controllo;
- una unità di controllo (15) ricevente in ingresso i dati provenienti dal dispositivo di rilevamento (9) e comprendente mezzi atti a discriminare i frame di controllo dai frame di informazione;
- una unità (16) di datazione collegata all'unità di controllo (15) e tale da associare un istante temporale di rilevamento ai frame di controllo ed ai frame di informazione;
- una unità (17) di memorizzazione di dati

discriminati atta a memorizzare i frame di controllo, i frame di informazione e l'istante temporale di rilevamento degli stessi, collegata in maniera bidirezionale all'unità di controllo (15); e

- una unità (18) di memorizzazione di dati predeterminati, collegata in maniera bidirezionale all'unità di controllo (15), detti dati predeterminati rappresentando possibili interpretazioni dei frame di informazione o di controllo contenuti nell'unità (17) di memorizzazione di dati discriminati ed essendo atti ad essere confrontati, tramite l'unità di controllo (15), con i dati contenuti nella parte di corpo dei frame di informazione o di controllo memorizzati nell'unità (17) di memorizzazione di dati discriminati, in maniera tale da permettere:

- un ordinamento temporale e secondo il tipo di comunicazione delle parti di corpo dei frame di controllo e di informazione; e

- una ricostruzione di alberi applicativi arricchiti di informazioni di tipo statistico secondo il tipo di comunicazione, in maniera da permettere certificazione delle comunicazioni ed il rilevamento di eventuali anomalie.

11. Dispositivo di controllo di accessi secondo la rivendicazione 10, caratterizzato dal fatto che il



dispositivo (9) di rilevamento dati comprende:

- un ricevitore dei dati di sorgente (12);
- un ricevitore dei dati di destinazione (13); e
- una interfaccia di connessione (14) atta a ricevere i segnali provenienti dal ricevitore dei dati di sorgente (12) e dal ricevitore dei dati di destinazione (13) ed a trasmettere gli stessi verso l'unità di controllo (15).

12. Dispositivo di controllo di accessi secondo la rivendicazione 10 o 11, caratterizzato dal fatto che la ricostruzione di detto albero applicativo arricchito di informazioni di tipo statistico avviene tramite confronto reciproco di ciascuna parte di corpo dei frame di informazione con le altre.

13. Dispositivo di controllo di accessi secondo una qualsiasi delle rivendicazioni da 10 a 12, caratterizzato dal fatto che la ricostruzione di detto albero applicativo arricchito di informazioni di tipo statistico avviene tramite confronto di ciascuna sequenza di parti di corpo dei frame di informazione con un insieme di sequenze predeterminate, rappresentanti possibili interpretazioni di sequenze di frame di informazione o di controllo contenuti nell'unità (17) di memorizzazione di dati discriminati, dette sequenze predeterminate essendo

contenute in detta unità (18) di memorizzazione di dati predeterminati.

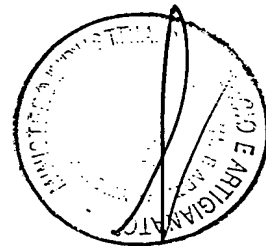
14. Dispositivo di controllo di accessi secondo una qualsiasi delle rivendicazioni da 10 a 13, caratterizzato dal fatto che detta unità (16) di datazione è di tipo a tempo assoluto, in particolare via radio o satellitare.

15. Dispositivo di controllo di accessi sostanzialmente come descritto in precedenza con riferimento ai disegni annessi.

p.p. ALASI di Arcieri Franco & C. s.a.s.

*Giorgio Strini*  
(Iscr. Albo n. 452 BM)

*WFW*



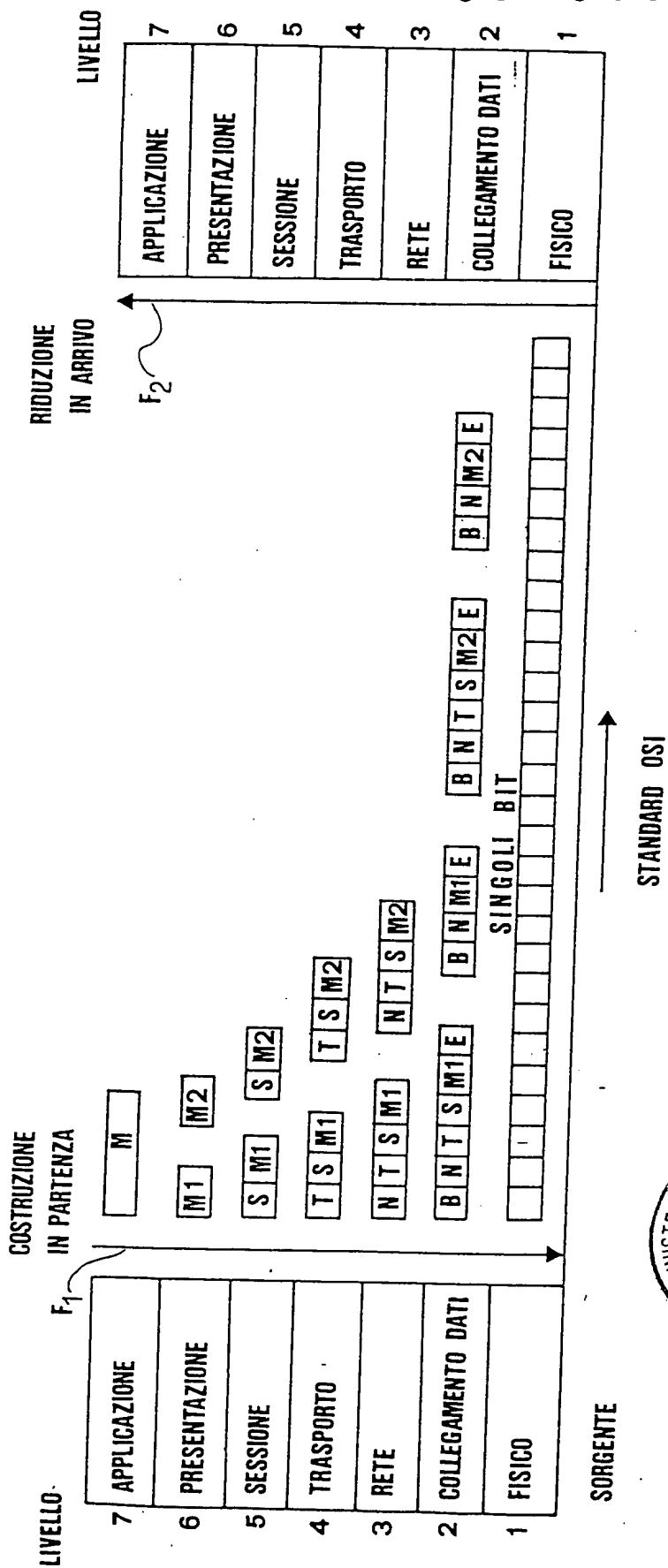
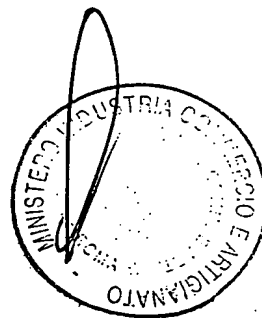


FIG 1



Giorgio Strini  
(Iscr. Albo n. 452 BM)

RM 98 A 000542

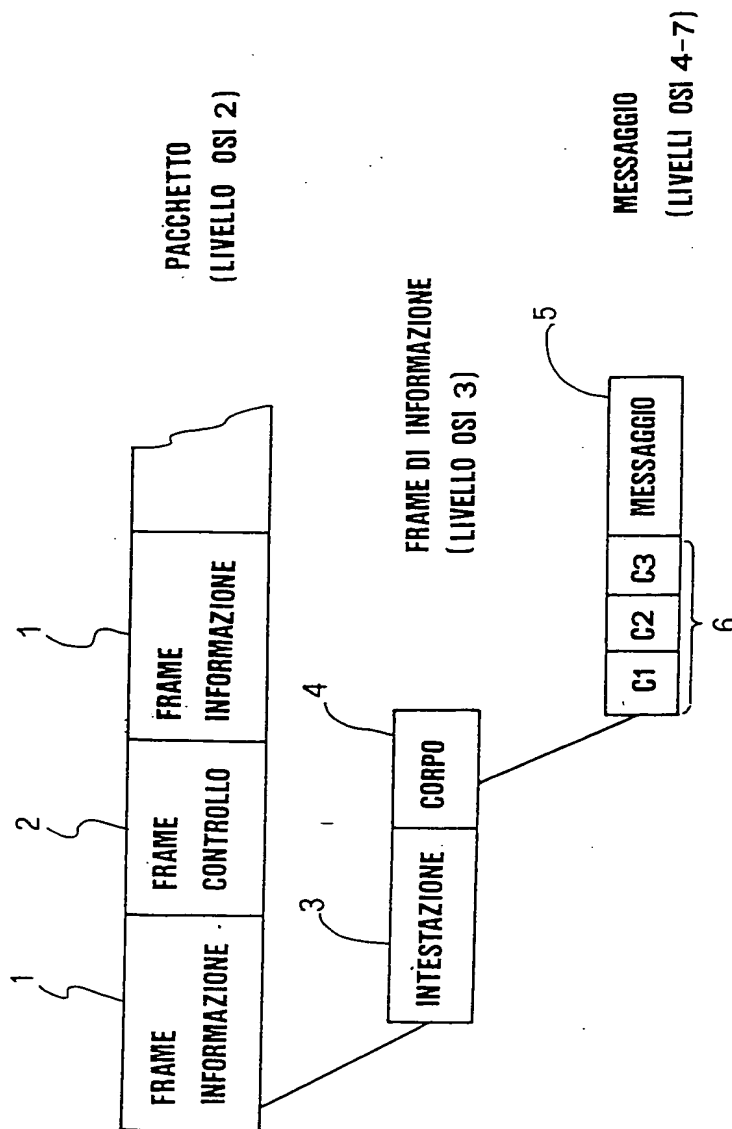
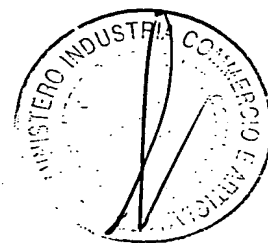


FIG 2



**Giorgio Strini**  
(Isr. Albo n. 452 BM)

p.p. ALASI di Arcieri Franco & C. s.a.s.

*Strini*

RM 98 A 000 542

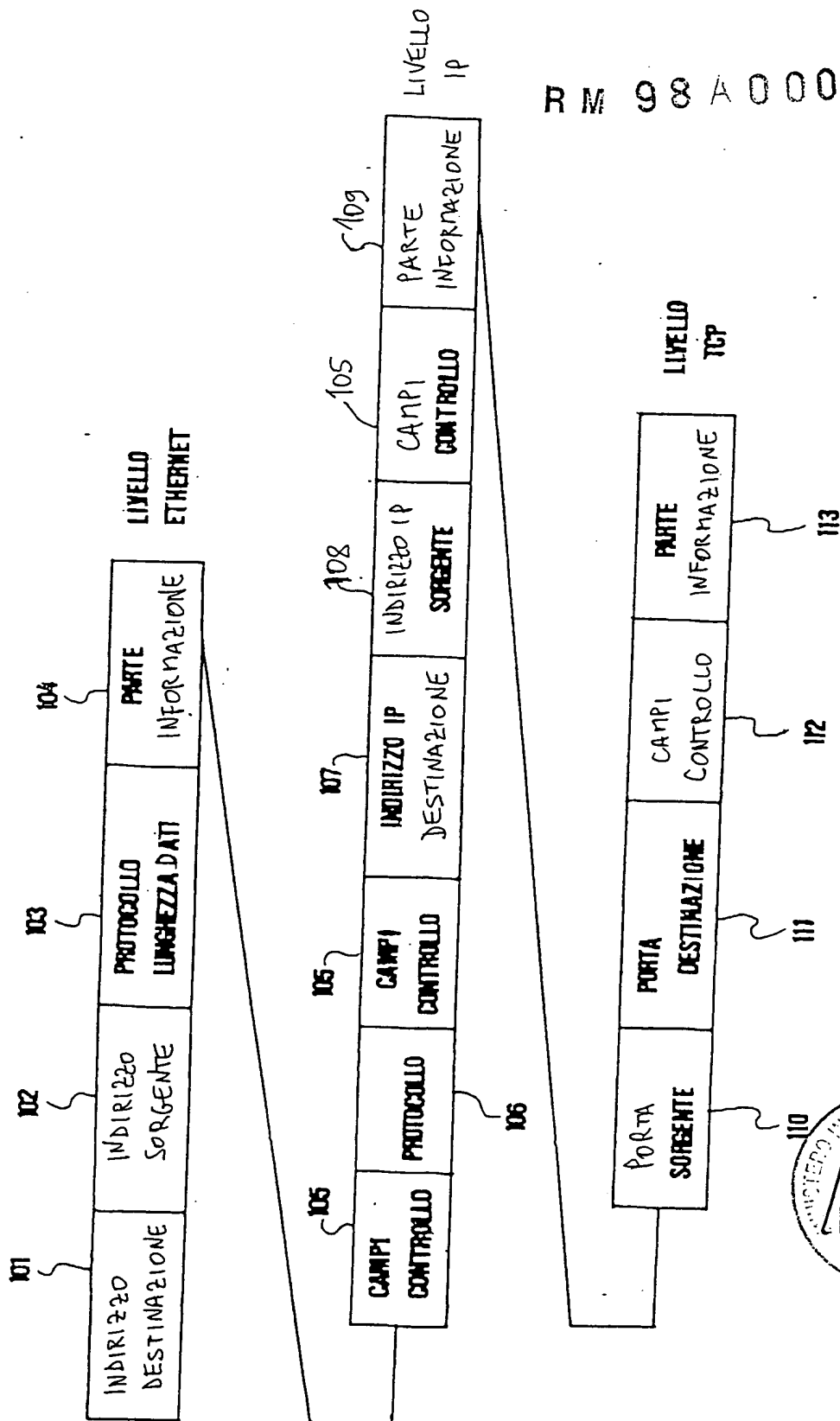
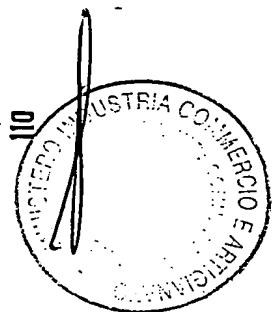


FIG. 3



Giorgio Strini  
(Iscr. Albo n. 452 BM)

RM 98 A 000542

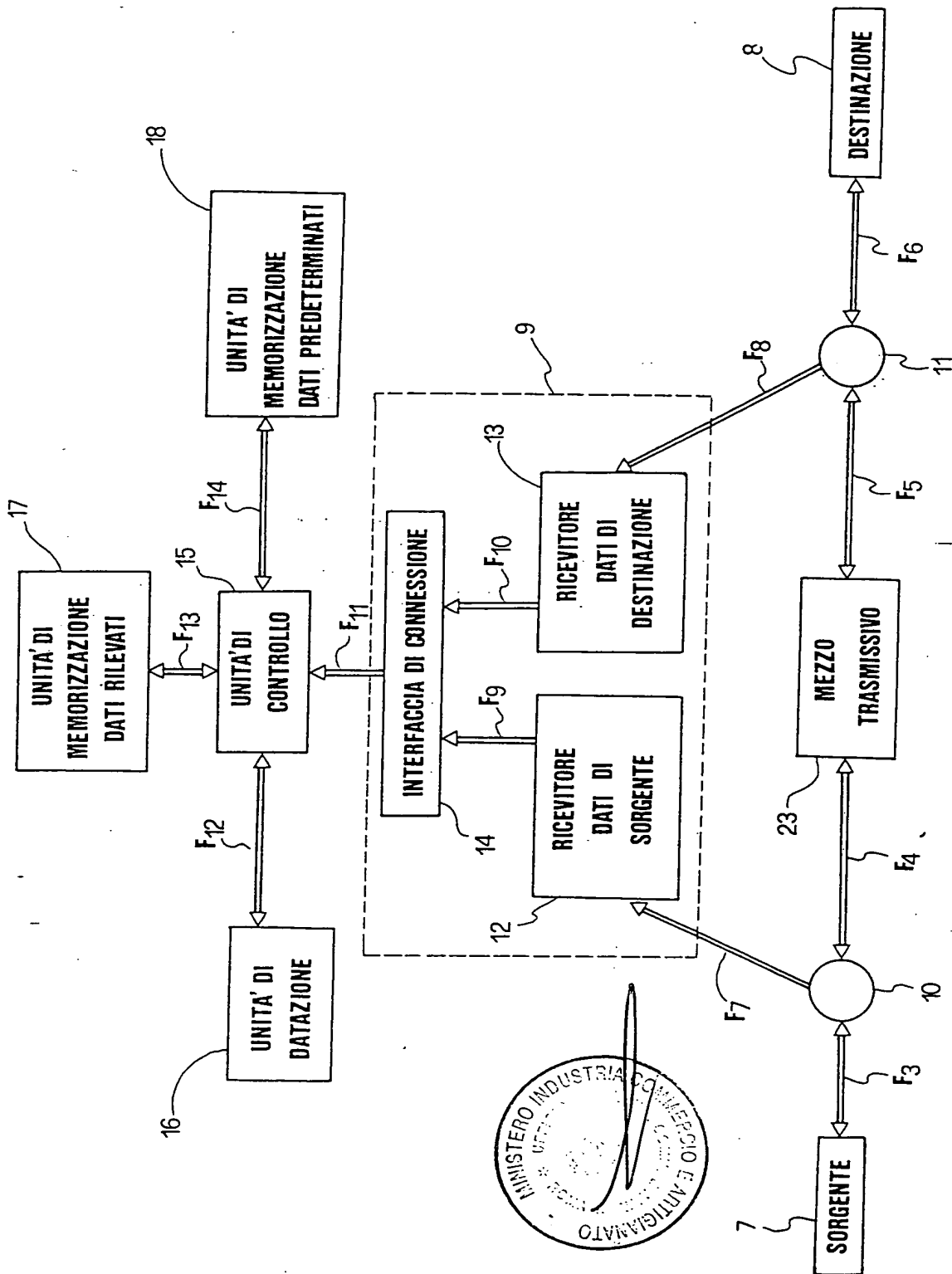
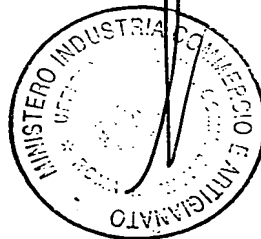
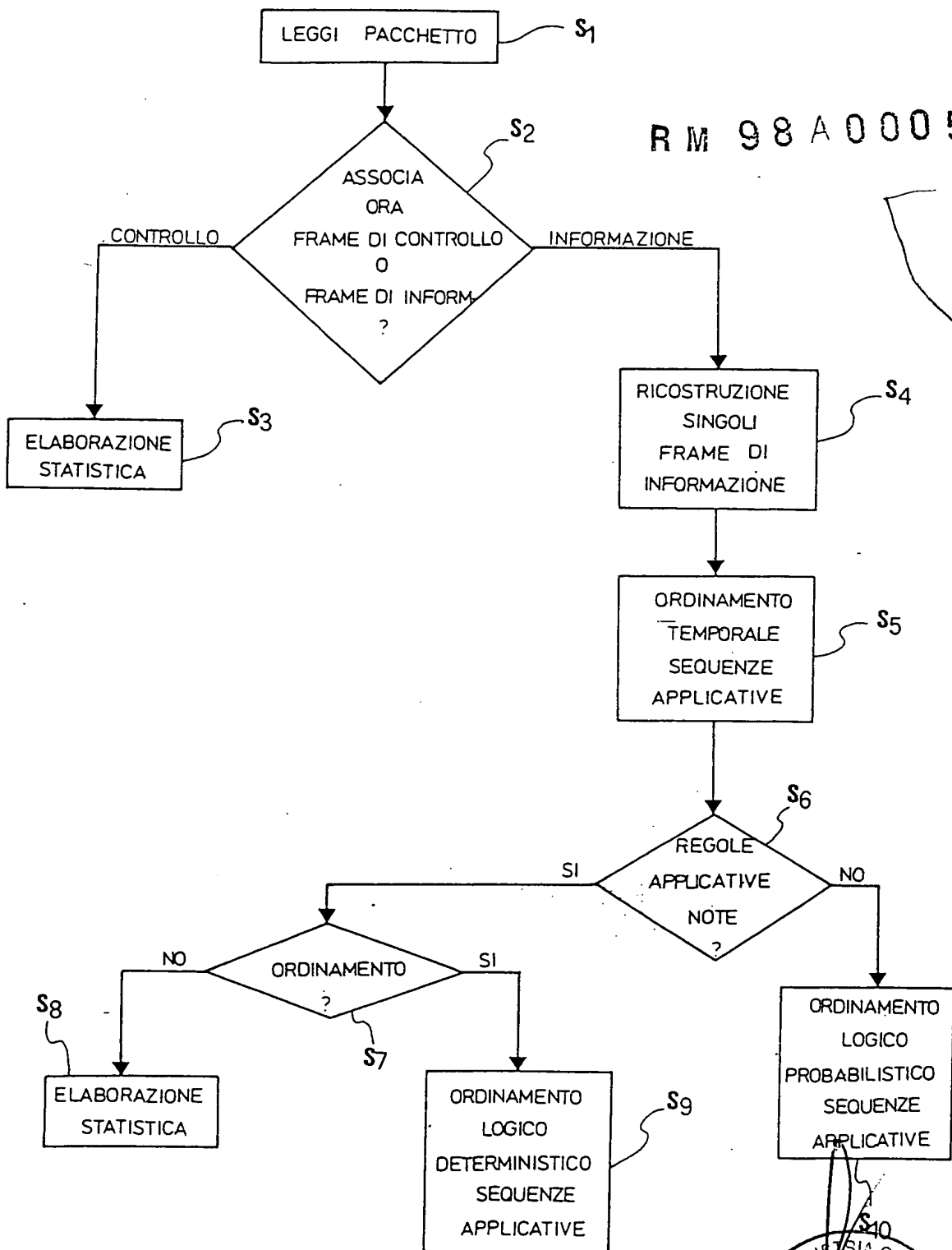


FIG. 4



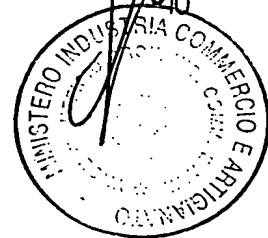
Giorgio Strini  
(Isr. Albo n. 452 BM)



RM 98 A 000542

FIG. 5

Giorgio Strini  
(Iscri. Albo n. 452 BM)



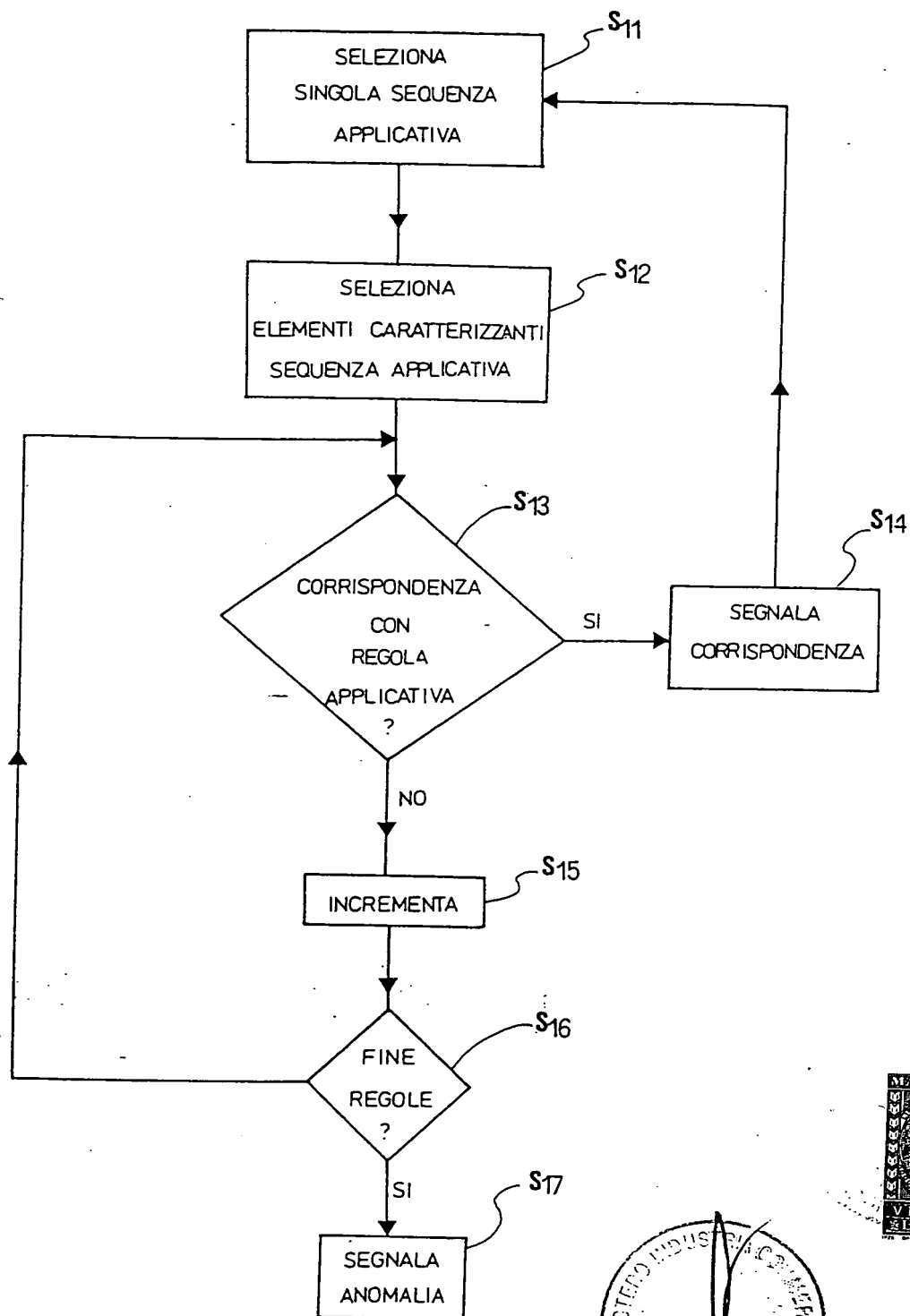
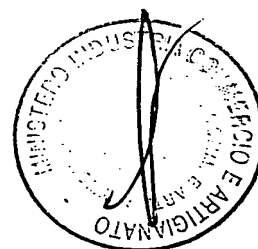


FIG. 6

Giorgio Strini  
(Iscr. Albo n. 452 BM)



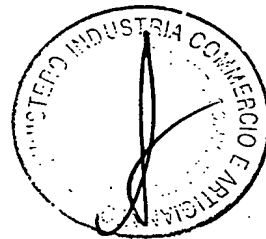
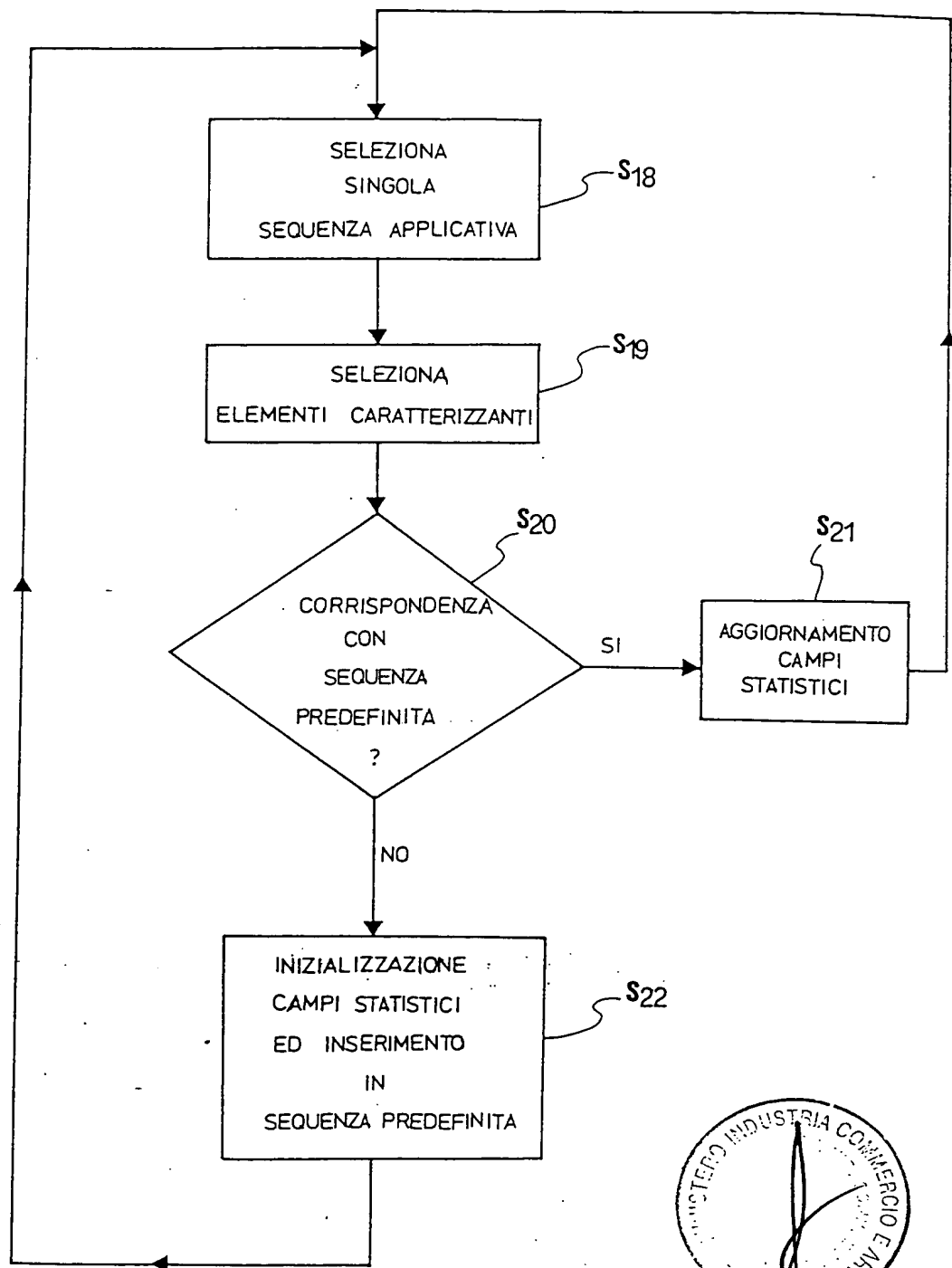


FIG. 7

Giorgio Strint  
(Iscr. Albo n. 452 BM)

RM 98 A 000542

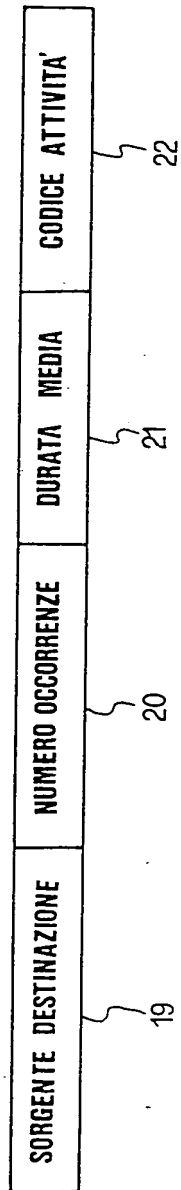


FIG. 8A

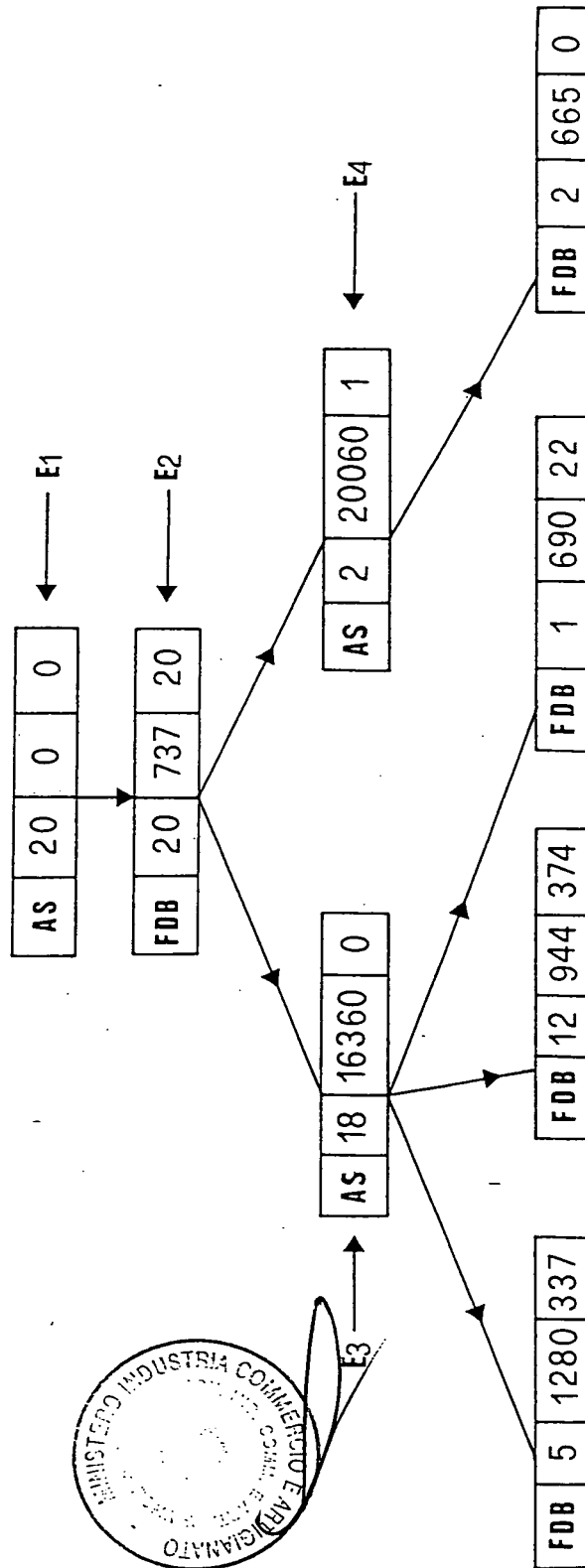


FIG. 8B

Giorgio Strini  
(Iscr. Albo n. 452 BM)



RM 98 A 000542

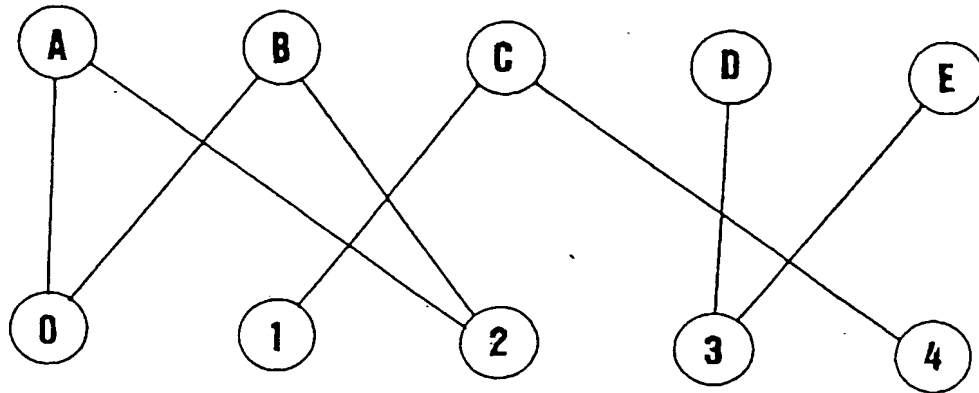
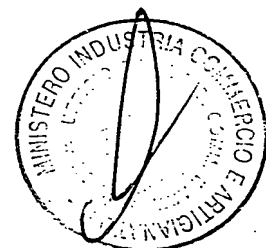


FIG. 10A

	0	1	2	3	4
A	x		x		
B	x		x		
C		x			x
D			x		
E			x		

FIG. 10B



Giorgio Strini  
(Iscri. Albo n. 452 BM)

*Strini*

RM 98 A 000542

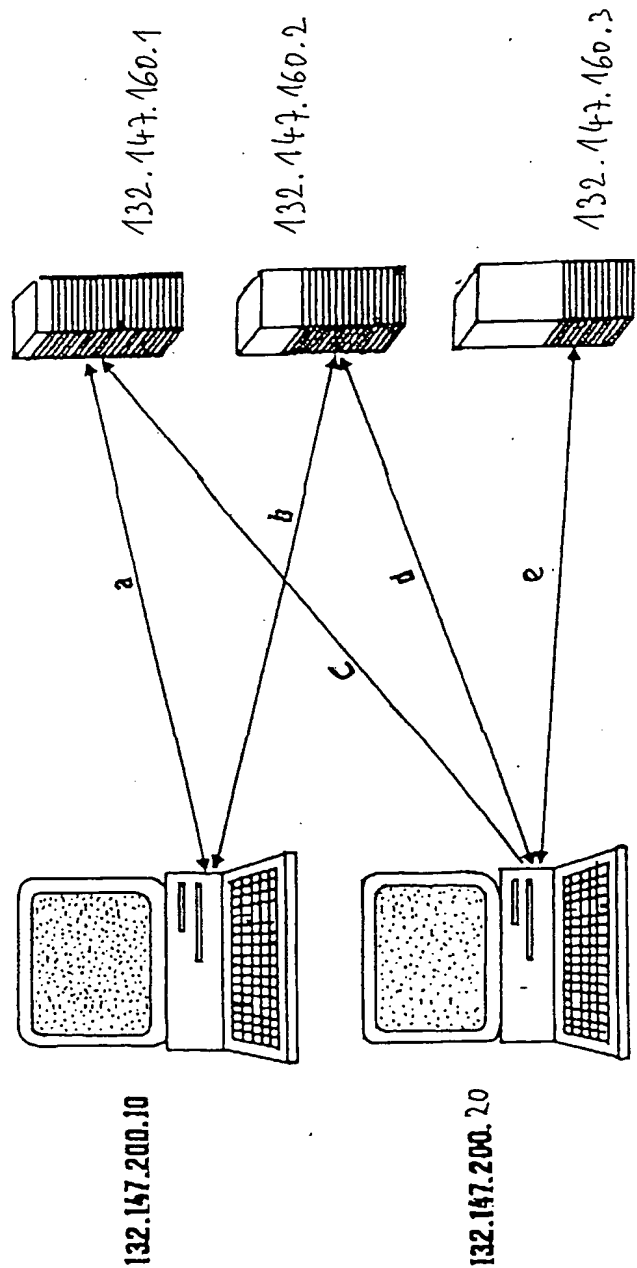
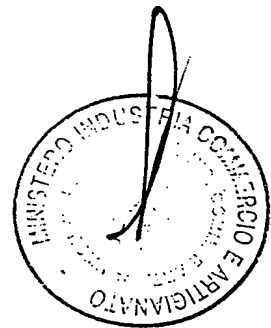


Fig. 11



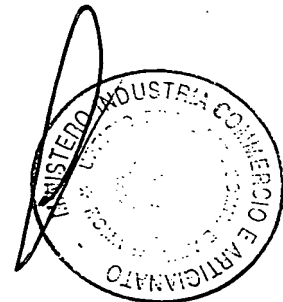
Giorgio Strini  
(Iscr. Albo n. 452 BM)

*Strini*

0	1	2	3	4	5	6	7	8	9	0A	0B	0C
1: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (01,4013) (00,8002) (50,8003)												
2: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (02,4013) (00,8002) (19,8003)												
3: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (02,4013) (00,8002) (89,8003)												
4: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (02,4013) (00,8002) (8A,8003)												
5: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (02,4013) (00,8002) (8B,8003)												
6: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (01,4013) (00,8002) (14,8003)												
7: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (01,4013) (00,8002) (15,8003)												
8: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (01,4013) (00,8002) (17,8003)												
9: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (02,4013) (00,8002) (19,8003)												
0A: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (02,4013) (00,8002) (50,8003)												
0B: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (03,4013) (00,8002) (50,8003)												
0C: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (03,4013) (00,8002) (A1,8003)												
0D: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (03,4013) (00,8002) (A2,8003)												
0E: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (03,4013) (08,8002) (01,8003)												
0F: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (03,4013) (00,8002) (17,8003)												
10: (08,000C) (06,000D)												
11: (08,000C) (00,000D) (01,4009)												

RM 98 A 000542

FIG. 12



Giorgio Strini  
(Iscr. Albo n. 452 BM)

p.p. ALASI di Arcieri Franco & C. s.a.s.

*Strini*

## AL MINISTERO DELL'INDUSTRIA DEL COMMERCIO E DELL'ARTIGIANATO

UFFICIO ITALIANO BREVETTI E MARCHI - ROMA

DOMANDA DI BREVETTO PER INVENZIONE INDUSTRIALE, DEPOSITO RISERVE, ANTICIPATA ACCESSIBILITÀ AL PUBBLICO

MODULO A



## A. RICHIEDENTE (I)

1) Denominazione ALASI di Arcieri Franco & C. s.a.s. SA  
 Residenza Austis (Nuoro), ITALIA codice 00915950919  
 2) Denominazione \_\_\_\_\_  
 Residenza \_\_\_\_\_ codice \_\_\_\_\_

## B. RAPPRESENTANTE DEL RICHIEDENTE PRESSO L'U.I.B.M.

cognome e nome de Benedetti Fabrizio ed altri cod. fiscale \_\_\_\_\_  
 denominazione studio di appartenenza SOCIETA' ITALIANA BREVETTI S.p.A.  
 via Piazza di Pietra n. 0039 città ROMA cap 00186 (prov) RM

## C. DOMICILIO ELETTIVO destinatario

via \_\_\_\_\_ n. \_\_\_\_\_ città \_\_\_\_\_ cap \_\_\_\_\_ (prov) \_\_\_\_\_

## D. TITOLO

classe proposta (sez/cl/sci)

gruppo/sottogruppo

"DISPOSITIVO DI CONTROLLO DI ACCESSI IN RETE TRAMITE IL RICONOSCIMENTO VELOCE DI TRAME APPLICATIVE CHE SODDISFANO UN INSIEME DI REGOLE PREDEFINITE"

ANTICIPATA ACCESSIBILITÀ AL PUBBLICO: SI ☐ NO ☒

SE ISTANZA: DATA \_\_\_\_/\_\_\_\_/\_\_\_\_

N° PROTOCOLLO \_\_\_\_\_

## E. INVENTORI DESIGNATI

cognome nome

cognome nome

1) ARCIERI Franco 3) TALAMO Maurizio  
 2) MARINELLI Guido Maria 4) \_\_\_\_\_

## PRIORITY

nazione o organizzazione

tipo di priorità

numero di domanda

data di deposito

allegato  
S/R

## SCIoglimento RISERVE

Data

N° Protocollo

1) \_\_\_\_\_  
 2) \_\_\_\_\_

## G. CENTRO ABILITATO DI RACCOLTA COLTURE DI MICRORGANISMI, denominazione

## H. ANNOTAZIONI SPECIALI

## DOCUMENTAZIONE ALLEGATA

N. es.

Doc. 1) 12) PROV n. pag. 85 riassunto con disegno principale, descrizione e rivendicazioni (obbligatorio 1 esemplare) \_\_\_\_\_  
 Doc. 2) 12) PROV n. tav. 12 disegno (obbligatorio se citato in descrizione, 1 esemplare) \_\_\_\_\_  
 Doc. 3) 10) RIS lettera d'incarico, ~~mod. 101~~ \_\_\_\_\_  
 Doc. 4) 10) RIS designazione inventore \_\_\_\_\_  
 5) 10) RIS documenti di priorità con traduzione in italiano \_\_\_\_\_  
 Doc. 6) 10) RIS autorizzazione o atto di cessione \_\_\_\_\_  
 Doc. 7) 10) nominativo completo del richiedente \_\_\_\_\_

SCIoglimento RISERVE	
Data	N° Protocollo
9 OTT. 1998	RM 1099
9 OTT. 1998	RM 1099

confronta singole priorità

8) attestati di versamento, totale lire novemcentoquindicimila=

obbligatorio

COMPILATO IL 12/08/1998 FIRMA DEL (I) RICHIEDENTE (I)

CONTINUA SU NO

Giorgio Strini  
 (Isr. Albo n. 452 BM)

DEL PRESENTE ATTO SI RICHIEDE COPIA AUTENTICA SU SI

UFFICIO PROVINCIALE IND. COMM. ART. DI

VERBALE DI DEPOSITO NUMERO DI DOMANDA

L'anno millenovecento novantottoil giorno dodici

del mese di

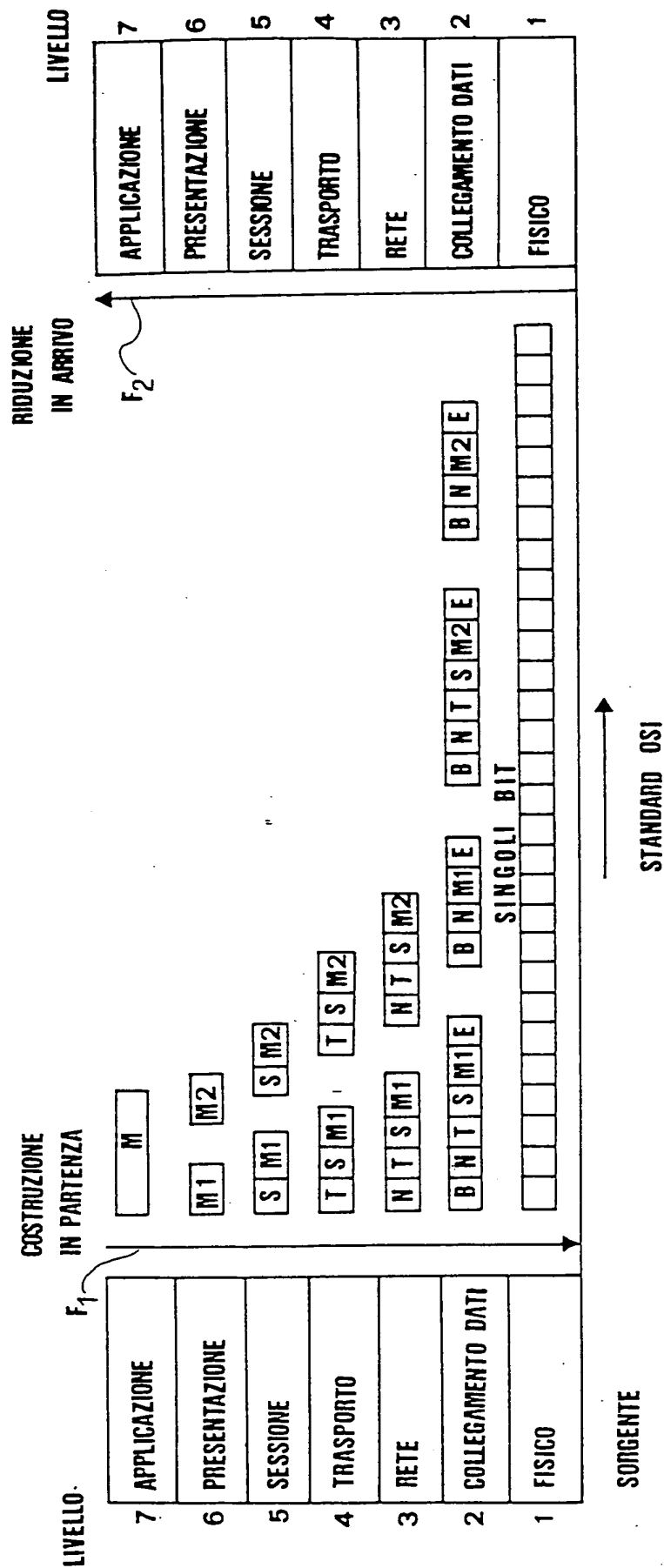
agostoil (i) richiedente (i) sopradicato (i) ha (hanno) presentato a me sottoscritto la presente domanda, corredata di n. 00 fogli aggiuntivi per la concessione del brevetto sopraportato.

## I. ANNOTAZIONI VARIE DELL'UFFICIO ROGANTE

IL DEPOSITANTE

timbro  
dell'ufficio

L'UFFICIALE ROGANTE  
 CESARE  
 Funzionario



R M R 10 99

FIG.1



*[Handwritten signature]*

R M R 10 99

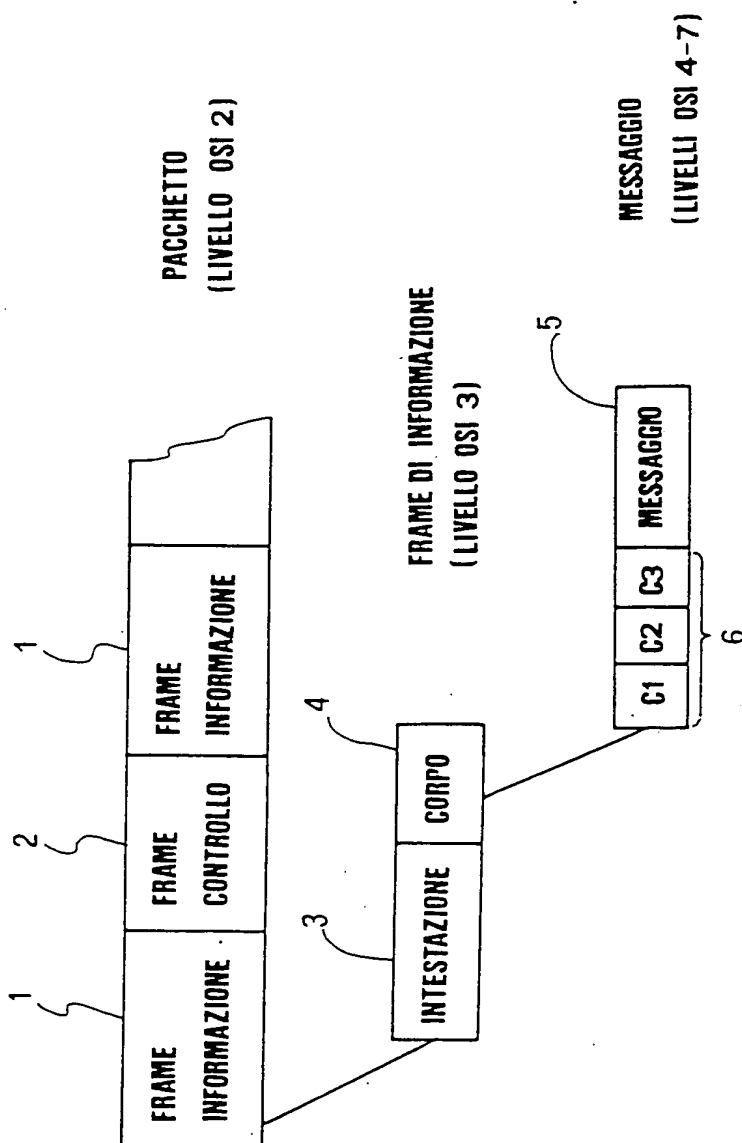
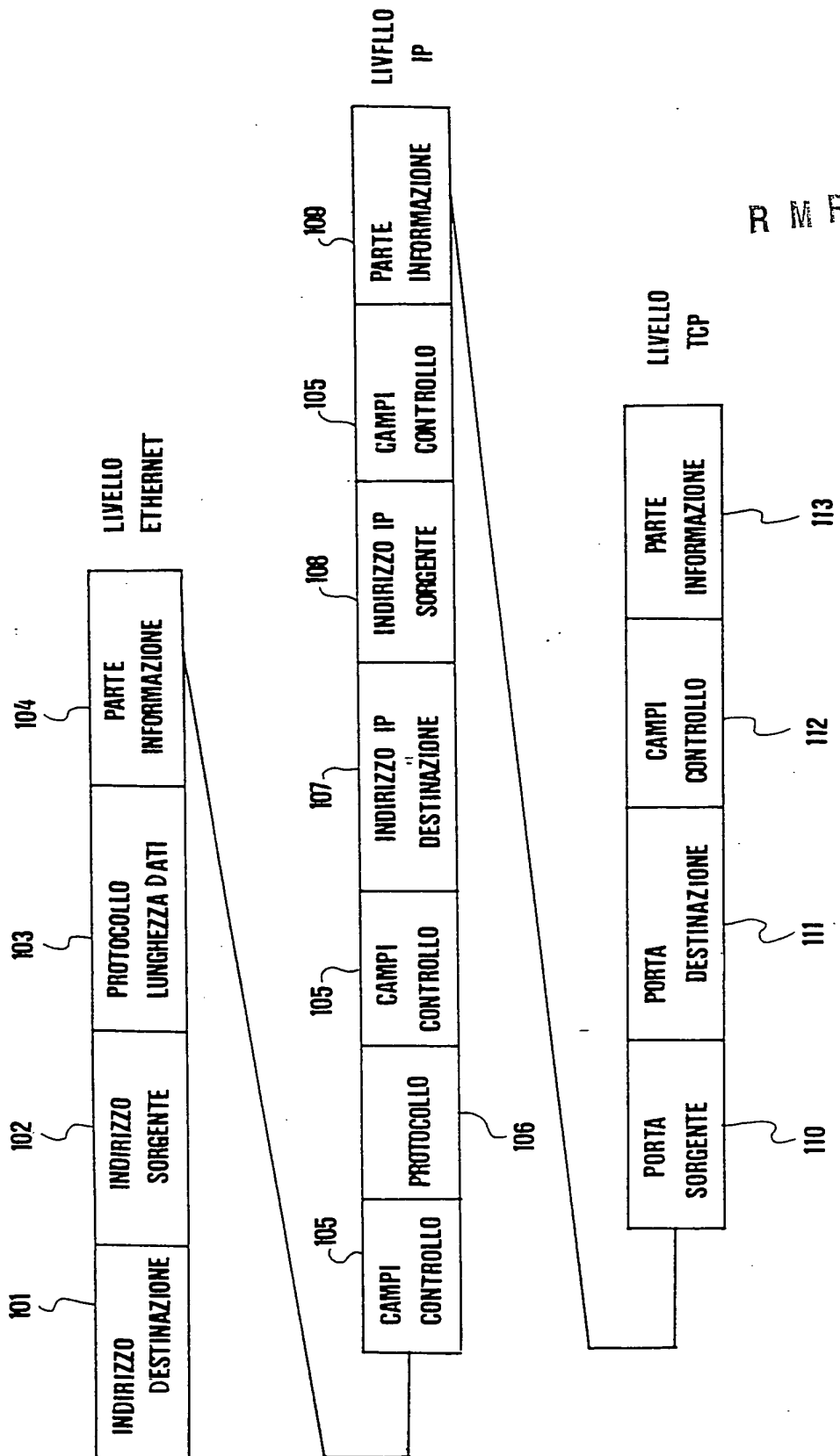


FIG.2



*[Handwritten signature]*



R M R 1099

FIG.3



R M R 10 99

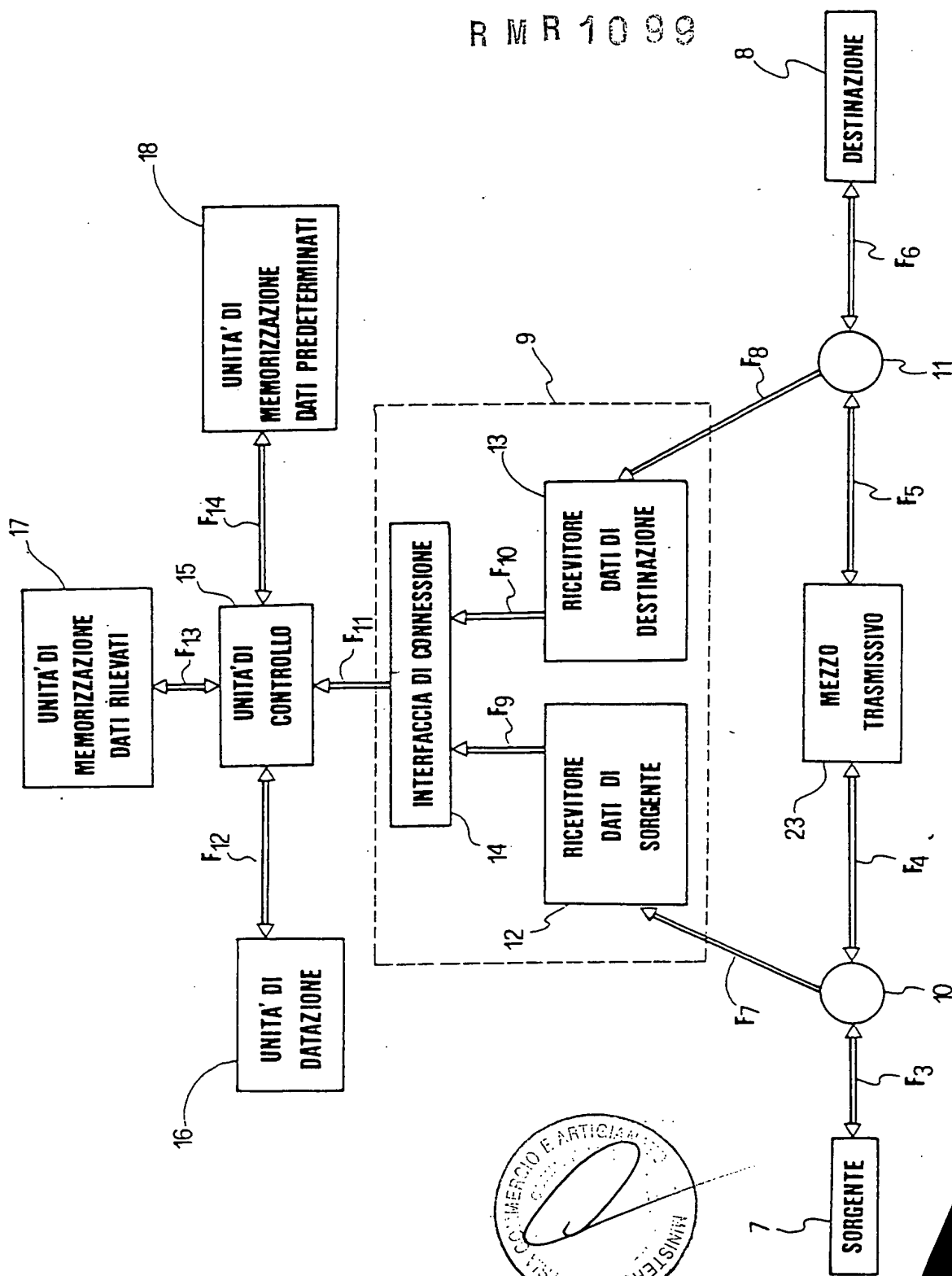


FIG.4



Gilberto Tonon  
(ref. Albo n. 83 BM)

R M R 1099

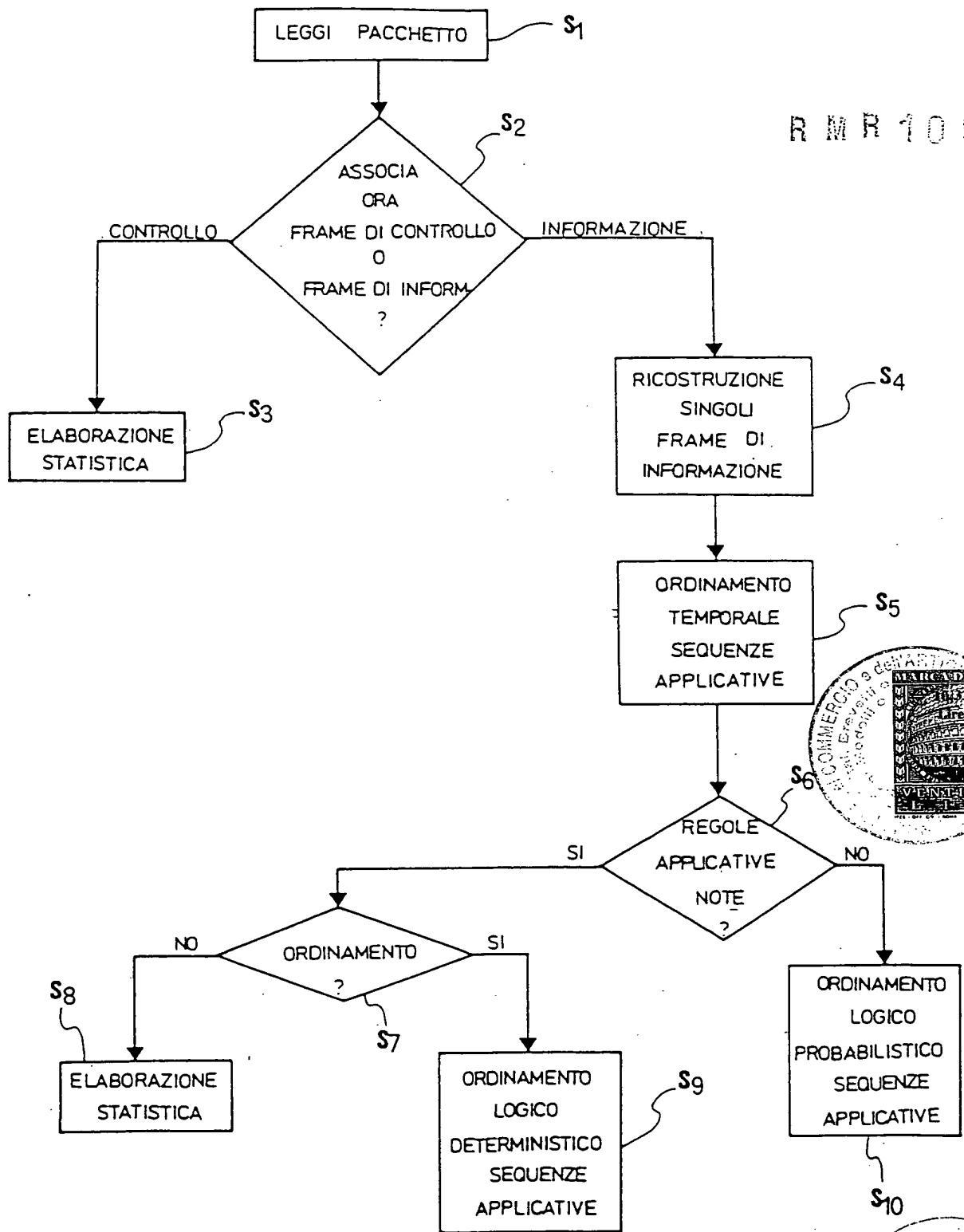


FIG.5

*[Handwritten signature]*

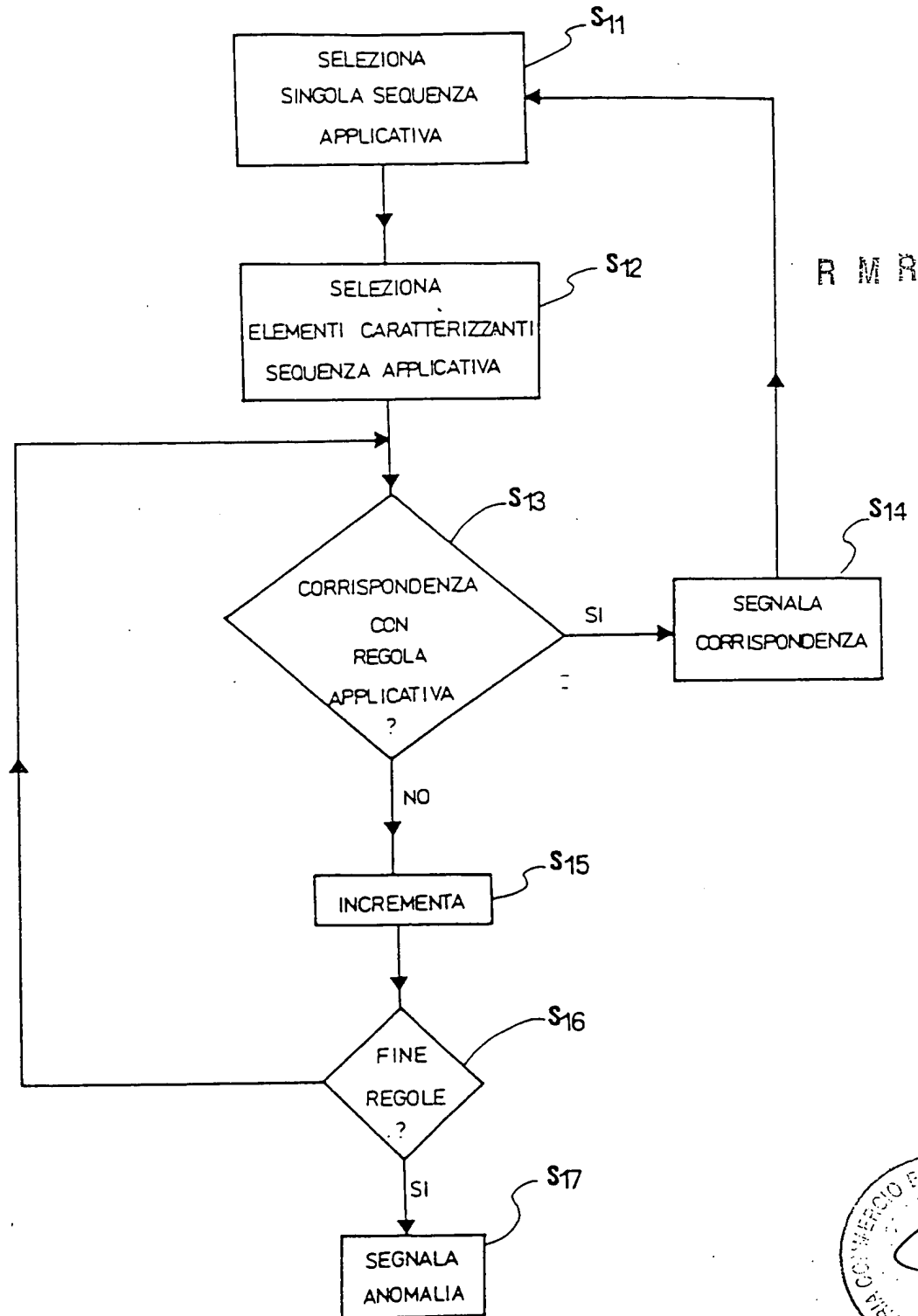


FIG. 6



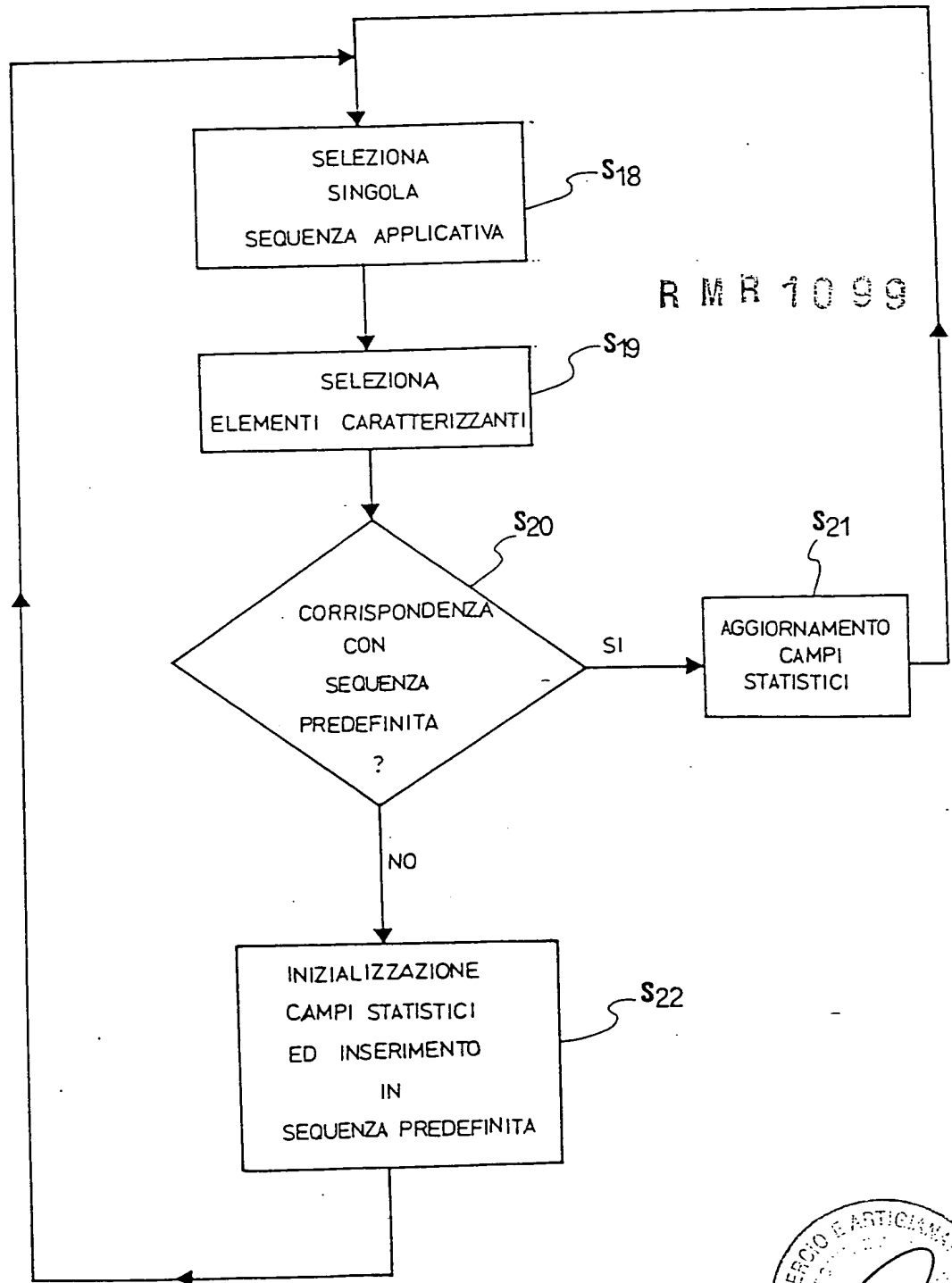


FIG.7



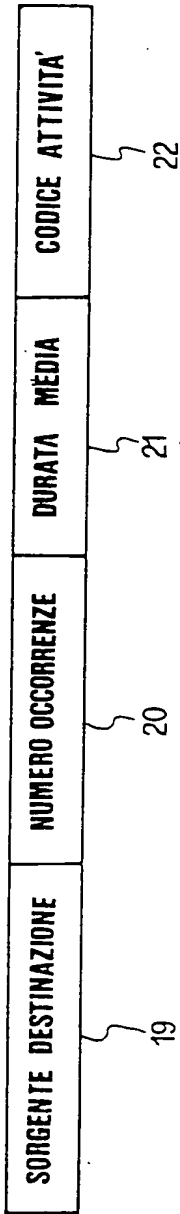


FIG.8A

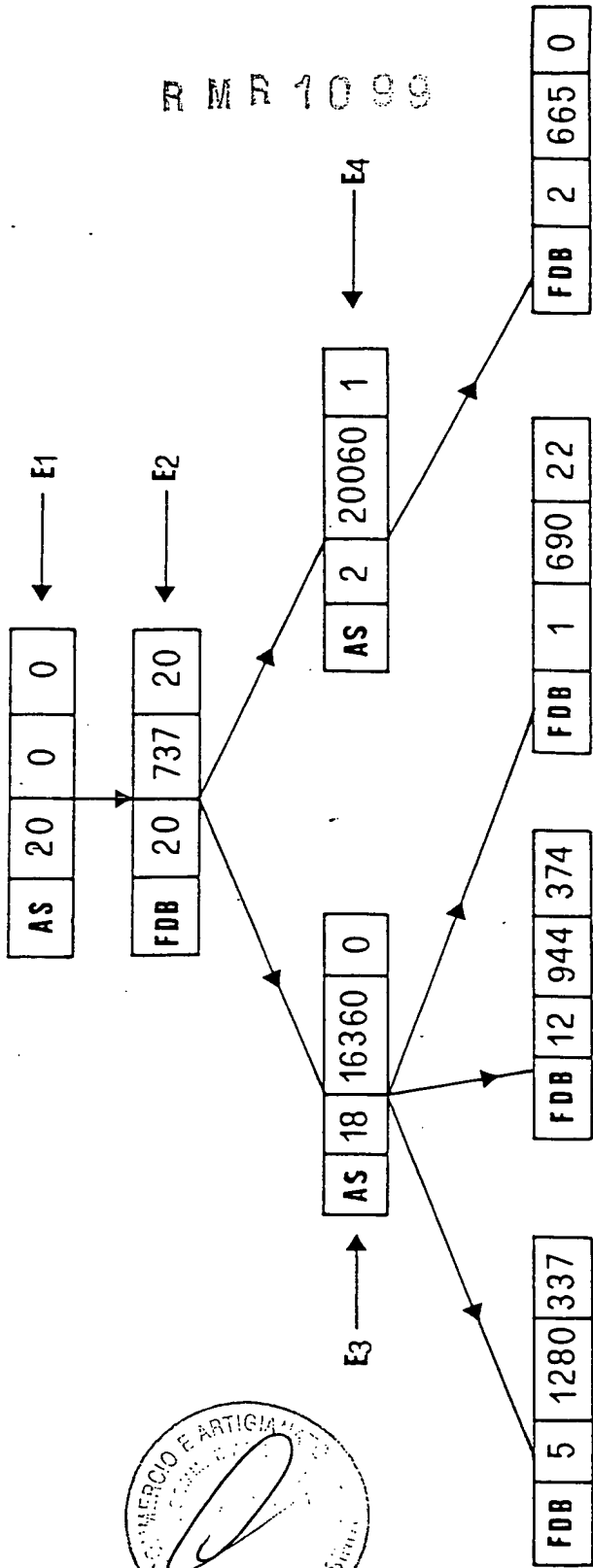
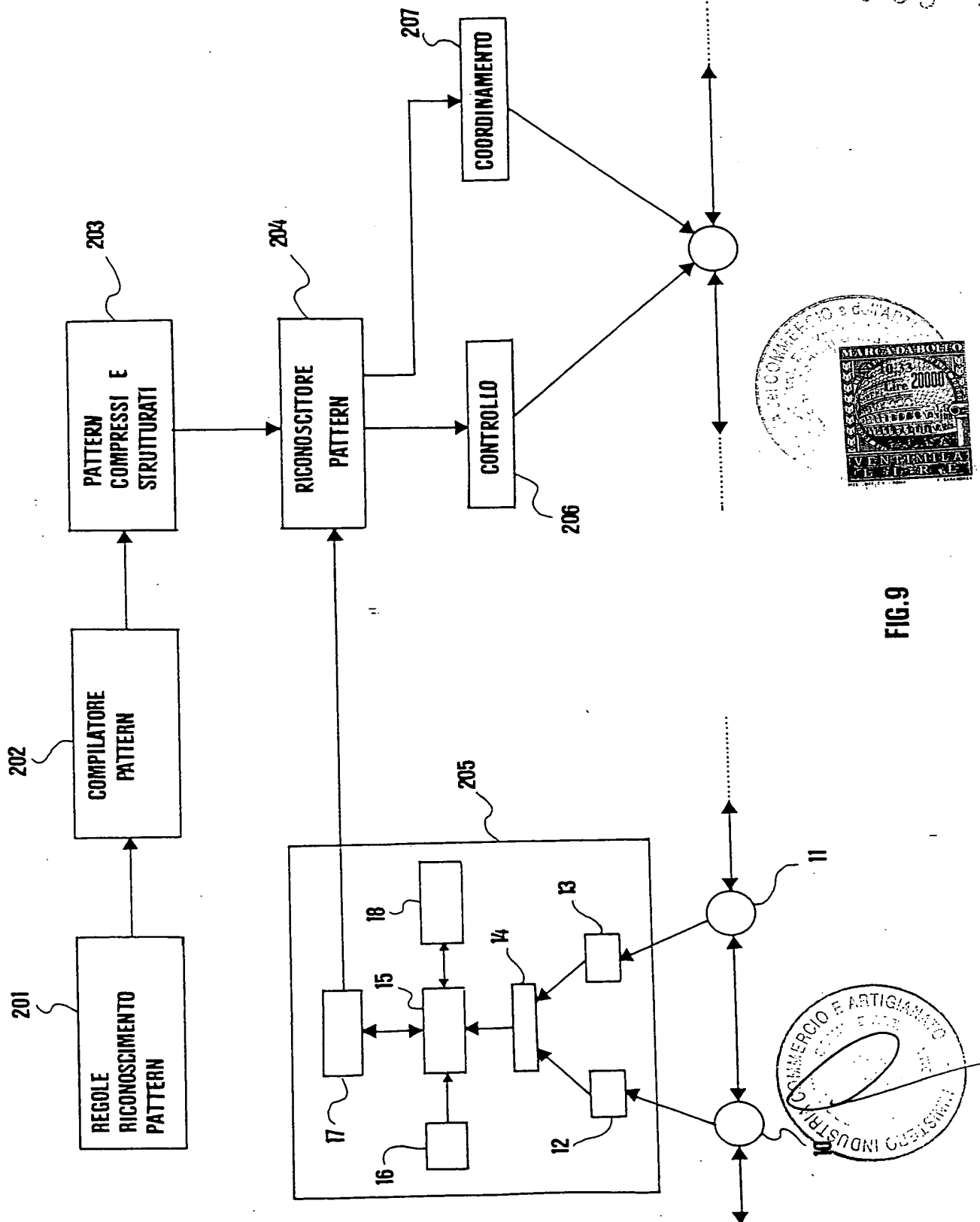


FIG.8B



R M R 10 99

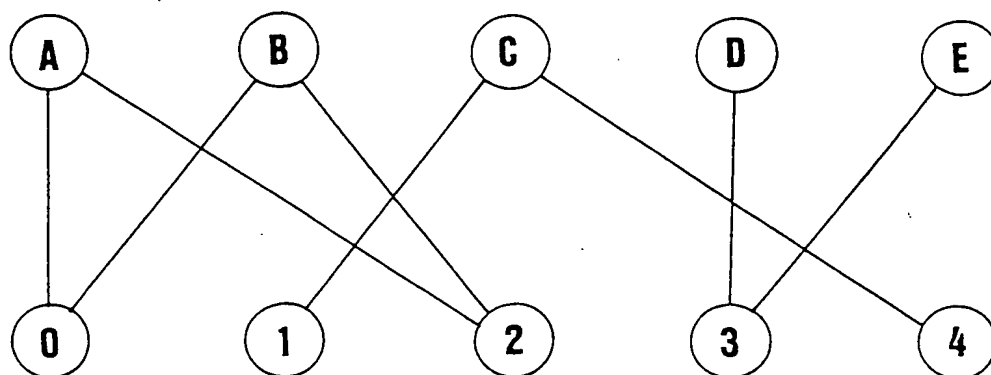


FIG.10A

	0	1	2	3	4
A	x		x		
B	x		x		
C		x			x
D			x		
E			x		

FIG. 10B



A handwritten signature in black ink, appearing to be "Tonon".

R M R 10 99

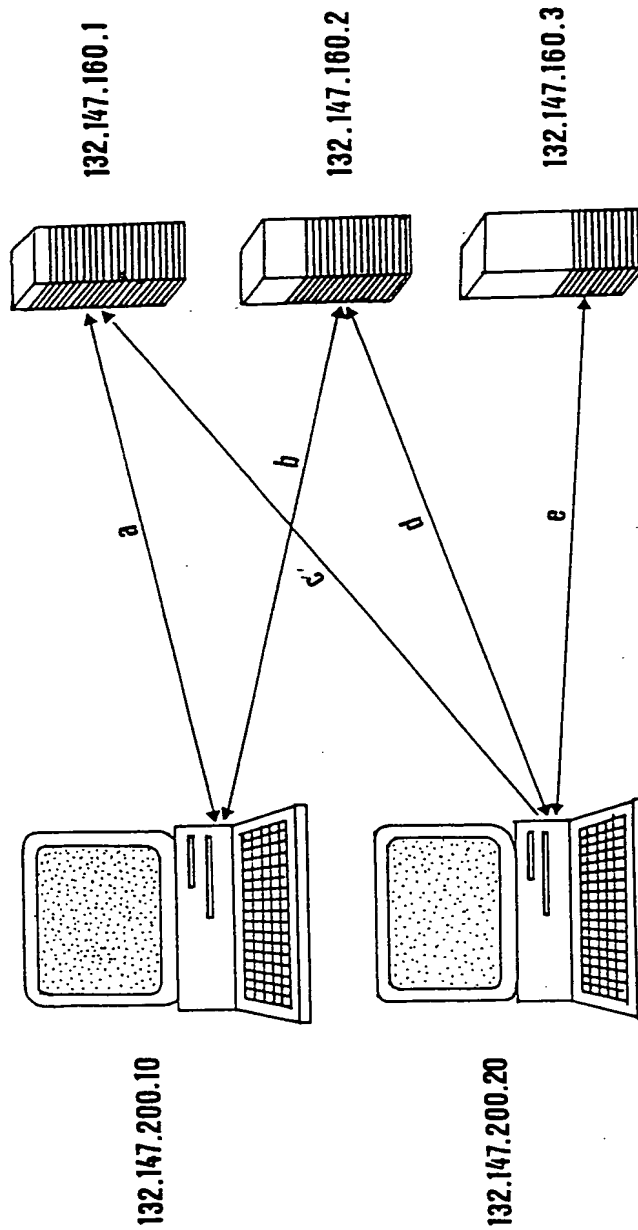


FIG.11



0	1	2	3	4	5	6	7	8	9	0A	0B	0C
1: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (01,4013) (00,8002) (50,8003)												
2: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (02,4013) (00,8002) (19,8003)												
3: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (02,4013) (00,8002) (89,8003)												
4: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (02,4013) (00,8002) (8A,8003)												
5: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (0A,400F) (84,4010) (93,4011) (A0,4012) (02,4013) (00,8002) (8B,8003)												
6: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (14,400F) (84,4010) (93,4011) (A0,4012) (01,4013) (00,8002) (14,8003)												
7: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (14,400F) (84,4010) (93,4011) (A0,4012) (01,4013) (00,8002) (15,8003)												
8: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (14,400F) (84,4010) (93,4011) (A0,4012) (01,4013) (00,8002) (17,8003)												
9: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (14,400F) (84,4010) (93,4011) (A0,4012) (02,4013) (00,8002) (19,8003)												
0A: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (14,400F) (84,4010) (93,4011) (A0,4012) (02,4013) (00,8002) (50,8003)												
0B: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (14,400F) (84,4010) (93,4011) (A0,4012) (03,4013) (00,8002) (50,8003)												
0C: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (14,400F) (84,4010) (93,4011) (A0,4012) (03,4013) (00,8002) (A1,8003)												
0D: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (14,400F) (84,4010) (93,4011) (A0,4012) (03,4013) (00,8002) (A2,8003)												
0E: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (14,400F) (84,4010) (93,4011) (A0,4012) (03,4013) (08,8002) (01,8003)												
0F: (08,000C) (00,000D) (06,4009) (84,400C) (93,400D) (C8,400E) (14,400F) (84,4010) (93,4011) (A0,4012) (03,4013) (00,8002) (17,8003)												
10: (08,000C) (06,000D)												
11: (08,000C) (00,000D) (01,4009)												

R M R 10 99

FIG.12



